Honeywell

HX3 Wearable Computer

User's Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

Web Address: www.honeywellaidc.com

Patents

For patent information, please refer to www.hsmpats.com.

Table of Contents

Chapter 1 - HX3 Agency Compliance

Chapter 2 - Getting Started

Chapter 3 - Hardware Configuration

Chapter 4 - Power Modes and Batteries

Chapter 5 - Software Configuration

Chapter 6 - Bluetooth Configuration

Chapter 7 - Bar Code Scanner Wedge

Chapter 8 - Enabler Installation and Configuration

Chapter 9 - Wireless Network Configuration

Chapter 10 - KeyMap

Chapter 11 - Desktop Cradle

Chapter 12 - Battery Charger

Chapter 13 - Specifications and Reference Material

Chapter 14 - Customer Support

1

HX3 Agency Compliance

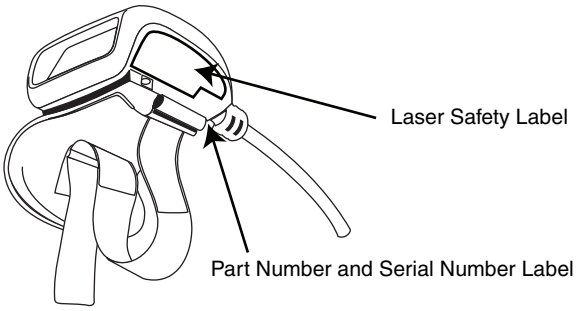
HX3 mobile voice computers meet or exceed the requirements of all applicable standards organizations for safe operation. However, as with any electrical equipment, the best way to ensure safe operation is to operate them according to the agency guidelines that follow. Read these guidelines carefully before using your HX3.

This documentation is relevant for the following models: HX3.

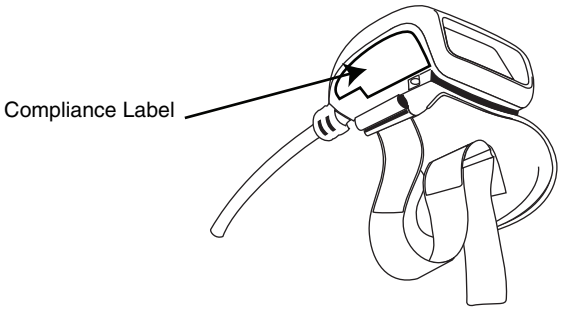
Caution: ⚠	RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. The battery should be disposed of by a qualified recycler or hazardous materials handler. Do not incinerate the battery or dispose of the battery with general waste materials.

Label Locations

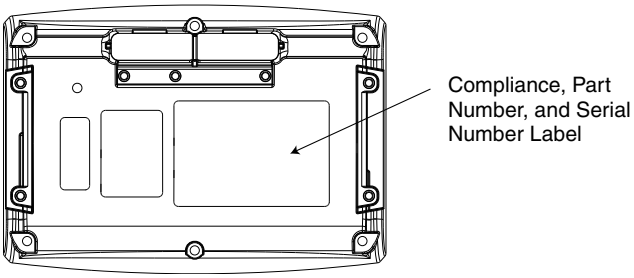
Left Side of Scanner head



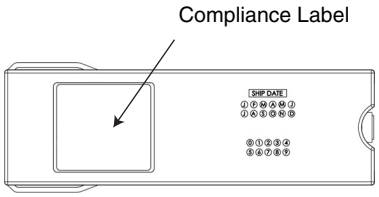
Right Side of Scanner Head



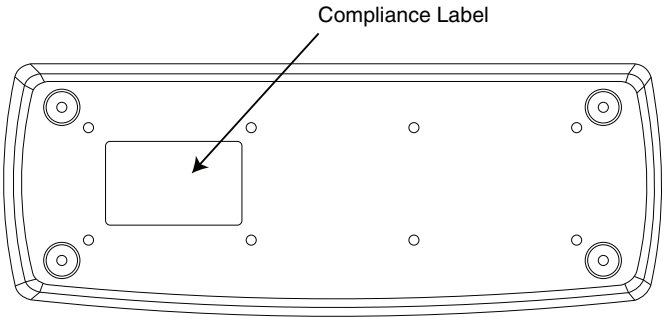
Back of HX3



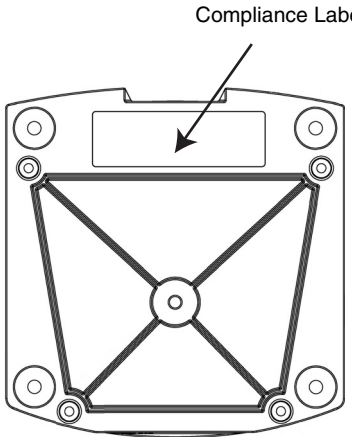
Battery



Bottom of Battery Charger



Bottom of Desktop Cradle

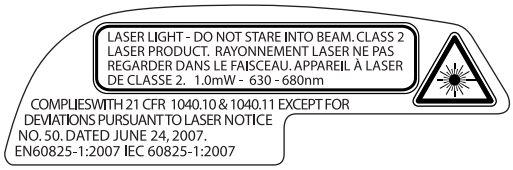


Laser Warnings

- Do not look into the laser's lens.
- Do not stare directly into the laser beam.
- Do not remove the laser caution labels from the tethered ring bar code decoder.
- Do not connect the laser bar code aperture to any other device. The laser bar code aperture is certified for use with the HX3 only.

Caution: 	Laser radiation when open. Read the caution labels. Use of controls, adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

If the following label is attached to your product, it indicates the HX3 tethered ring bar code decoders contain an engine with a laser aimer:

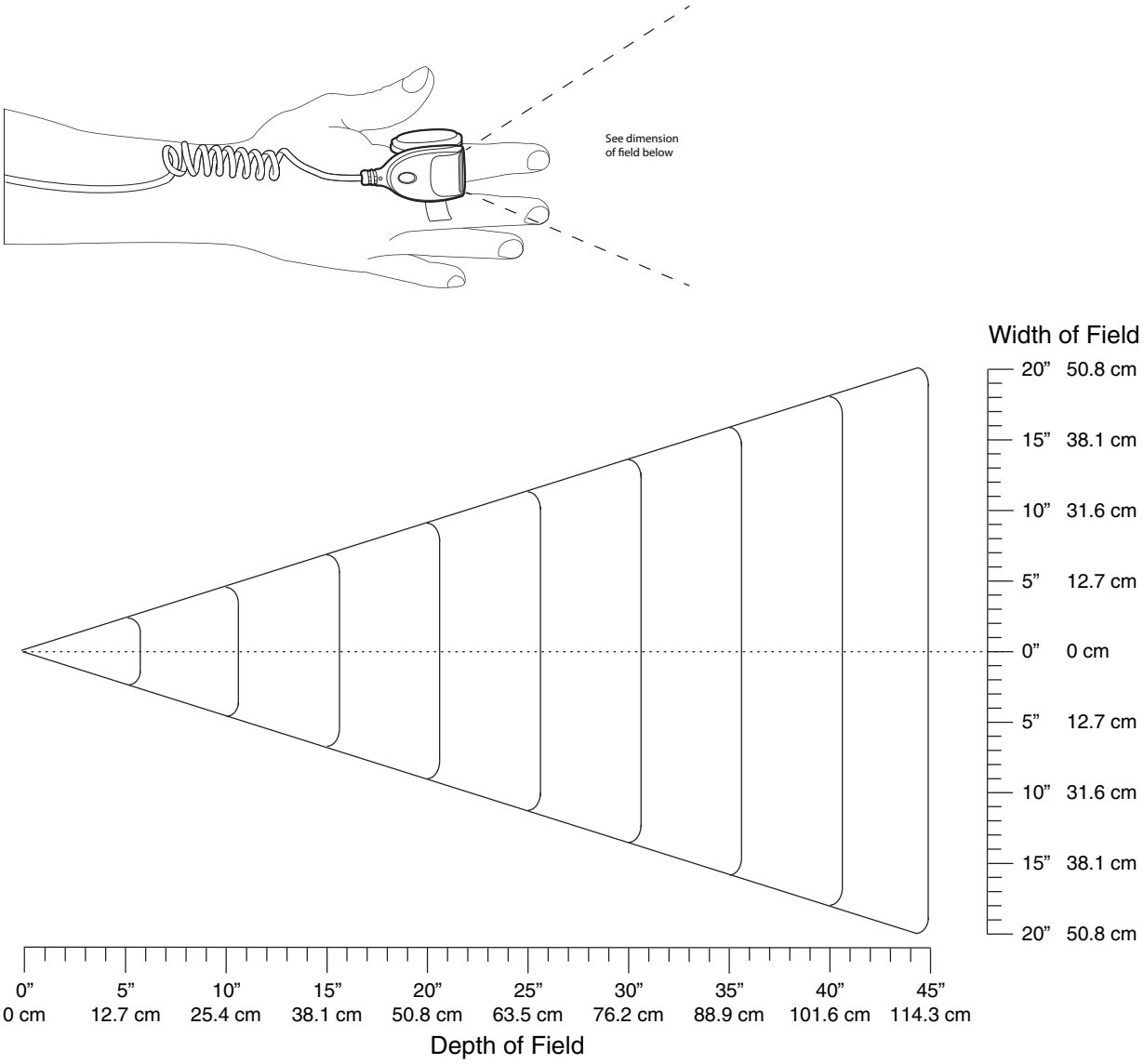


Laser Safety Statement

This device has been tested in accordance with and complies with IEC60825-1:2007 and EN60825-1:2007). Complies with 21 CFR 1040.10 and 1040.11, except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.

LASER LIGHT, DO NOT STARE INTO BEAM, CLASS 2 LASER PRODUCT, 1.0 mW MAX OUTPUT: 630-680nM.

Beam Divergence



FCC Part 15 Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet helpful: “Something About Interference.” This is available at FCC local regional offices. Honeywell is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Honeywell. The correction is the responsibility of the user.

Caution: Any changes or modifications made to this equipment not expressly approved by Honeywell may void the FCC authorization to operate this equipment.

FCC 5GHz Statement

LAN devices are restricted to indoor use only in the band 5150-5250 MHz. For the band 5600-5650 MHz, no operation is permitted.

When using IEEE 802.11a wireless LAN, this product is restricted to indoor use, due to its operation in the 5.15- to 5.25-GHz Frequency range. The FCC requires this product to be used indoors for the frequency range of 5.15 GHz to 5.25 GHz to reduce the potential for harmful interference to co-channel mobile satellite systems. High-power radar is allocated as the primary user of the 5.25- to 5.35-GHz and 5.65- to 5.85-GHz bands. These radar stations can cause interference with and/or damage to this device.

Canadian Compliance

This ISM device complies with Canadian RSS-210.

Operation is subject to the following conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

CE Mark

The CE marking indicates compliance with the following directives:

- 1995/5/EC R&TTE
- 2011/65/EU RoHS (Recast)

In addition, complies to 2006/95/EC Low Voltage Directive, when shipped with recommended power supply. European contact::

CE

Hand Held Products Europe BV
Nijverheidsweg 9-13
5627 BT Eindhoven
The Netherlands

Honeywell shall not be liable for use of our product with equipment (i.e., power supplies, personal computers, etc.) that is not CE marked and does not comply with the Low Voltage Directive.

RF Safety Notices

This device contains transmitter Module FCC ID: KDZLXE4830P.
Caution:
This portable device with its antenna complies with FCC and Industry Canada RF exposure limits set for an uncontrolled environment. This equipment has shown compliance with FCC and Industry Canada Specific Absorption Rate (SAR) limits. Highest reported SAR for the HX3 is 0.641W/kg on body. Any accessories not provided by Honeywell should not be used with this device. This device must not be co-located or operating in conjunction with any other antenna or transmitter.

This device contains transmitter Module FCC ID: KDZLXE4831P.
Caution:
This portable device with its antenna complies with FCC and Industry Canada RF exposure limits set for an uncontrolled environment. This equipment has shown compliance with FCC and Industry Canada Specific Absorption Rate (SAR) limits. Highest reported SAR for the HX3 is 0.333W/kg on body. Any accessories not provided by Honeywell should not be used with this device. This device must not be co-located or operating in conjunction with any other antenna or transmitter.

Bluetooth

Bluetooth® Class II

Honeywell Scanning & Mobility Product Environmental Information

Refer to www.honeywellaidc.com/environmental for the RoHS / REACH / WEEE information.

China RoHS

HX3 佩戴式数据终端 (Wearable Computer)

有毒有害物质名称及含量的标识 **(Names and Content of Hazardous Substances or Elements)**

部件名称 **(Parts Name)**	有毒有害物质或元素 **(Toxic and Hazardous Substances or Elements)**					
	铅 **(Pb)**	汞 **(Hg)**	镉 **(Cd)**	六价铬 **(Cr6+)**	多溴联苯 **(PBB)**	多溴二苯醚 **(PBDE)**
印刷电路部件 **(PCA)**	x	o	x	o	o	o
无綫通信设备 **(Wireless Communication Device)**	x	o	x	o	o	o
备份电池 **(Backup Battery)**	x	o	x	o	o	o
内部电缆 / 连接器 **(Internal Cables / Connectors)**	x	o	o	o	o	o

o: 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T11363-2006 标准规定的限量要求以下 (Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in China's SJ/T11363-2006)
x: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T11363-2006 标准规定的限量要求 (Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in China's SJ/T11363-2006)

HX3 指环扫描器 (Ring Scanner)

有毒有害物质名称及含量的标识 **(Names and Content of Hazardous Substances or Elements)**

部件名称 **(Parts Name)**	有毒有害物质或元素 **(Toxic and Hazardous Substances or Elements)**					
	铅 **(Pb)**	汞 **(Hg)**	镉 **(Cd)**	六价铬 **(Cr6+)**	多溴联苯 **(PBB)**	多溴二苯醚 **(PBDE)**
扫描模块 **(Scanner Module)**	x	o	o	o	o	o
印刷电路部件 **(PCA)**	x	o	o	o	o	o
外壳 **(Housing)**	x	o	o	o	o	o
连接线 **(Cable)**	x	o	o	o	o	o

o: 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T11363-2006 标准规定的限量要求以下 (Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in China's SJ/T11363-2006)
x: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T11363-2006 标准规定的限量要求 (Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in China's SJ/T11363-2006)

Dealer License - Republic of Singapore

Complies with
IDA Standards
DA103458

2 Getting Started

Overview

The HX3 is a small, lightweight wearable voice computer. The HX3 is designed for use with voice applications while the user's hands are actively engaged with the physical environment, including piece picking to carts, containers or conveyers; case picking; parcel moves; and broken case activities.

The HX3 keypad is designed for use with voice applications. Because of the limited design, the HX3 should be connected via ActiveSync or Windows Mobile Device Center to a host computer running LXEConnect when a full keyboard is needed (for example, during system configuration). The HX3 does not have a touch screen. If the host computer has a touch screen, instructions using "tap" and "stylus" instead of "click" and "mouse" apply.

Note: Contact Customer Support (page 14-1) for upgrade availability if your application or control panels are not the same as the application or control panels presented in this guide.

The HX3 can be docked in a desktop cradle. The HX3 batteries can be re-charged while the HX3 is in the desktop cradle. The batteries are also re-charged in a Battery Charger. When the HX3 is docked in a powered desktop cradle, connection is broken between the tethered battery and the HX3. The HX3 begins receiving power through the powered desktop cradle connector. It may be necessary to wake the HX3 from Suspend when it is inserted in the desktop cradle.

About this Guide

This HX3 User's Guide provides instruction for the system administrator to follow when configuring a HX3. Also included are setup and use instructions for the Battery Charger and Desktop Cradle.

Out of the Box

After you open the shipping carton verify it contains the following items:

- HX3 wearable voice computer
- Rechargeable battery
- Quick Start Guide

If you ordered accessories for the HX3, verify they are also included with the order. Keep the original packaging material in the event the HX3 should need to be returned for service. For details, see Product Service and Repair (page 14-1).

Initial Setup for the HX3

Note: The HX3 does not have a touch screen. If the host computer has a touch screen, instructions using "tap" and "stylus" instead of "click" and "mouse" apply.

Note: ActiveSync or Windows Mobile Device Center must be installed on a host computer with a USB port.

1. Connect the HX3 using the USB-Client cable to the host computer.
2. Copy LXEConnect setup files from the HX3 to the host computer.
3. Install and launch LXEConnect on the host computer.
4. Accept the End User License Agreement (EULA).

When HX3 configuration is complete, exit LXEConnect on the host computer and disconnect the ActiveSync connection and cable. Contact Customer Support (page 14-1) if any of the above steps causes issues.

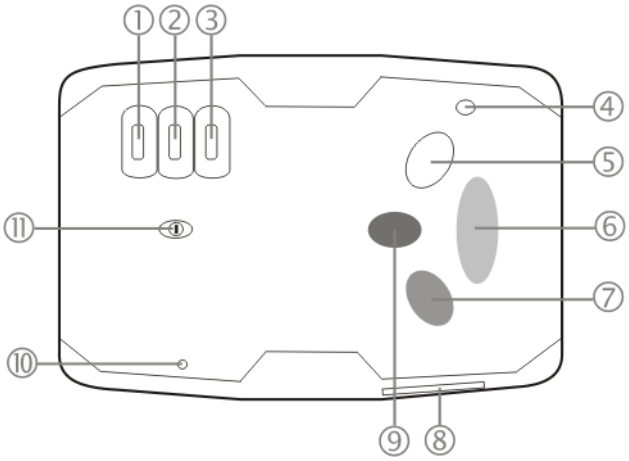
End User License Agreement (EULA)

When a new HX3 starts up a EULA is displayed. It remains active until the Accept or Decline button is clicked. Click the Accept button to accept the EULA terms and the HX3 continues the startup process. The EULA is not presented to the user again. Click the Decline button to decline the EULA and the HX3 will reboot. It will continue to reboot until the Accept button is clicked.

Note: The EULA will be presented after any operating system upgrade or re-installation, including language-specific operating systems.

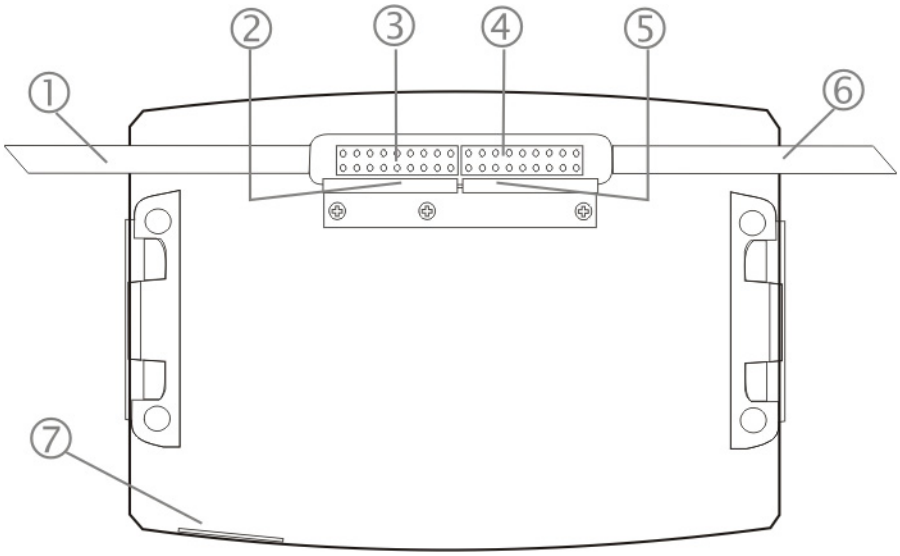
Components

Front View



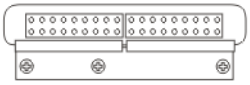
1. Wireless LED (Yellow)
2. Bluetooth LED (Blue)
3. System Status LED (Green or Red)
4. Speaker
5. White Button (Up Arrow)
6. Yellow Button (Enter)
7. Green Button (Down Arrow)
8. Cradle Connector
9. Blue Modifier Key
10. Microphone
11. Power Button

Back View



HX3 Worn on Left Side, Ring on Left Hand	HX3 Worn on Right Side, Ring on Right Hand
1. Ring Scanner Tether cable channel	1. Tethered Battery Cable channel
1. Retaining Clip for Ring Scanner Tether Connector	1. Retaining Clip for Tethered Battery Connector
1. Ring Scanner cable connector	1. Battery Cable connector
1. Battery Cable connector	1. Ring Scanner cable connector
1. Retaining Clip for Tethered Battery Connector	1. Retaining Clip for Ring Scanner Tether Connector
1. Tethered Battery Cable channel	1. Ring Scanner Tether cable channel
1. Cradle Connector	1. Cradle Connector

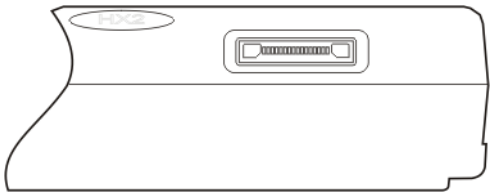
Ring Scanner / Audio / Battery Connectors



Connector 1 is on the left. Connector 2 is on the right. Both connect to cables for:

- Tethered Ring Scanner (Laser or Imager)
- Tethered Headset / Microphone and Battery
- Tethered Battery

Cradle Connector



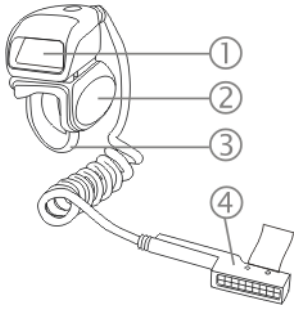
Connector 3 is at the base of the HX3. It connects to the Cradle. When the HX3 is in a powered desktop cradle, the HX3 receives external power through the cradle connector.

USB Keyboard or USB Mouse input is received by the HX3 through the cradle connector when the HX3 is in a powered desktop cradle.

Ring Scanner and Ring Imager

The trigger module and ring strap module are user replaceable

Laser Scanner.



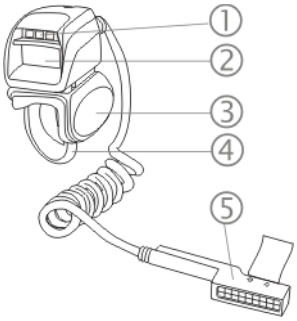
1. Scan Window
2. Trigger
3. Ring Strap
4. Connector (connect to HX3)

Continuous Scan Mode

If Continuous Scan Mode has been enabled (factory default setting is 'Disabled'), the laser (or imager) is always on and decoding.

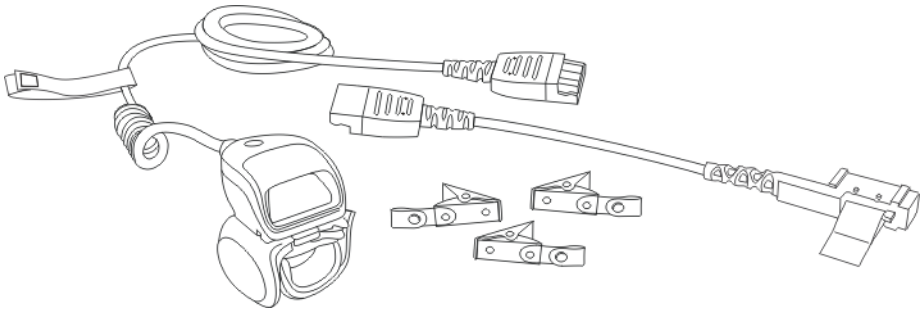
Caution: Laser beam is emitted continuously. Do not stare into the laser beam.

Laser Imager



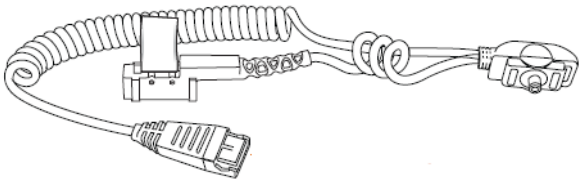
1. Illumination LEDs
2. Scan Window
3. Trigger
4. Ring Strap
5. Connector (Connect to HX3)

Ring Scanner and Ring Imager Extended Cable



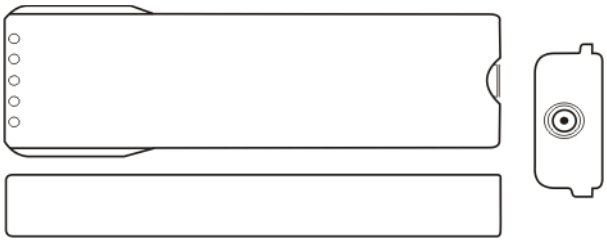
Clips are used to secure the cable to clothing. Wristband is used to secure the cable to the user's wrist.

Audio Connector and Battery Connection Cable

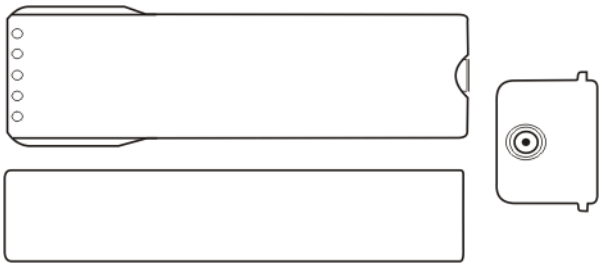


Li-Ion Battery

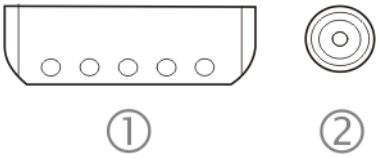
The HX3 cannot function unless a battery is securely tethered. Be sure to place the HX3 in Suspend mode before disconnecting a battery, or all unsaved data may be lost.



Standard Battery



Extended Battery



1. Battery Charge/Connect Terminals
2. Battery Cable Connector

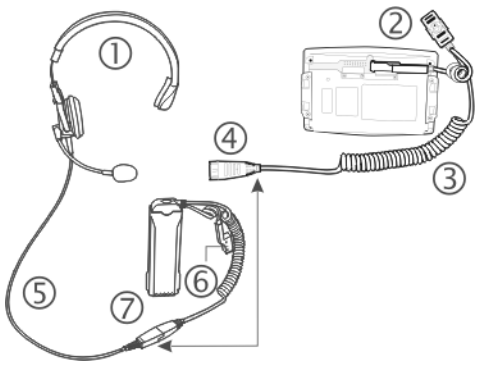
The Standard battery is much thinner than the Extended battery. Each battery will fit in the battery sleeve on body-worn cases.

When placing the tethered battery in a battery sleeve, ensure the Battery Charge/Connect terminals are protected from accidental damage by keeping them covered by the sleeve fabric at all times.

Do not allow water or chemical cleaning agents of any kind to come in contact with the battery charging contacts or the battery cable connector; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Assembling the HX3 Voice Computer and Accessories

Note: Installing or removing accessories should be performed on a clean, well-lit surface. When necessary, protect the work surface, the HX3, and components from electrostatic discharge.

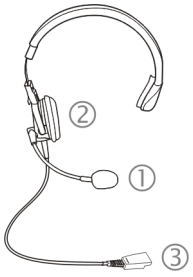


1. Headset
2. Connect To Battery
3. Audio Cable
4. Connect To Headset Cable
5. Headset Cable
6. Connect To HX3
7. Battery

1. Put the headset on.
2. Connect the headset cable (5) to the audio cable and battery connection cable (3).
3. Connect the battery connector end of the cable (3) to the battery (7).
4. Connect the audio cable end (6) to the back of the HX3.

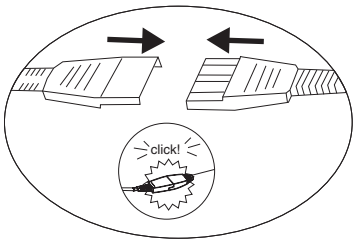
The following pages contain detailed installation instruction for the above steps.

Assembling the Headset Cable



1. Microphone
2. Headphones
3. Connects to voice cable end of voice cable

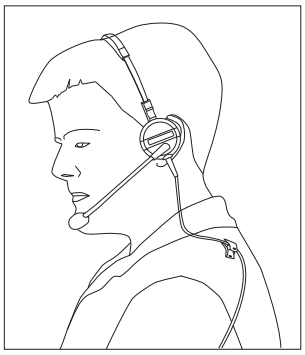
1. Connect the HX3 voice cable I/O connector to the I/O port on the HX3. The HX3 internal microphone and speaker are automatically disabled.



2. Slide the voice cable ends together until they click and lock in place. Do not twist or bend the connectors. The HX3 is ready for voice-enabled applications.

Adjusting Headset / Microphone and Securing Cable

The headset consists of an earpiece, a microphone, a clothing clip and a cable. The headset attaches to the audio cable end of the voice cable which attaches to the HX3.



Do not twist the microphone boom when adjusting the microphone. The microphone should be adjusted to be about two finger widths from your mouth.

Make sure the microphone is pointed at your mouth. Note the small “Talk” label near the mouthpiece. Make sure the Talk label is in front of your mouth. The microphone cable can be routed over or under clothing.

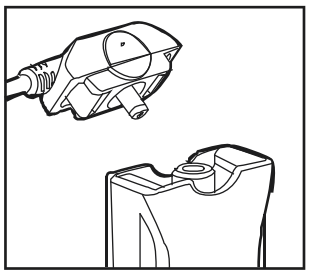
Under Clothing

Leave the cable exposed only at the top of the collar. Be sure to leave a small loop of cable to allow movement of your head.

Over Clothing

Use clothing clips to hold the cable close to your body. Tuck the cable under the belt, but leave a small loop where it goes under the belt. Do not wear the cable on the front of your body. It may get in your way or get caught on protruding objects.

Connecting the Cable to the Battery



To connect the cable to the battery, complete the following steps:

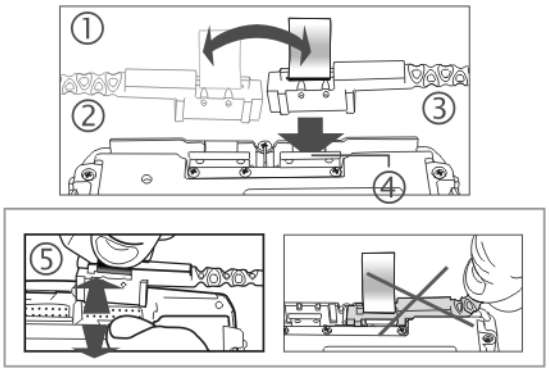
Hold the battery with one hand with the connector facing up.

3. Holding the battery connector cable end in your other hand, press the battery cable connector down onto the battery connector, making sure the connectors line up.

Connecting the Ring and Battery Cables

The battery cable and the ring scanner/imager cable should not be exchanged or replaced in a dirty, harsh or hazardous environment. When the tethers are disconnected, any dust or moisture that adheres to the tether connector can potentially cause damage upon cable re-connection.

Connecting the Battery Cable to the HX3

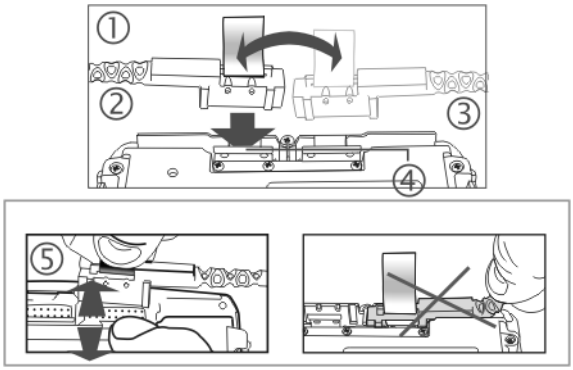


1. Connect
2. Armband Right Arm
3. Armband Left Arm
4. Press Down
5. Remove

When you want to switch connectors from left to right, or vice versa, first gently press downward on the Retaining Clip, then pinch and pull the cable connector (not the cable!) straight up and away from the HX3. Do not use a metal object, or extreme force, to remove the cable connector from the HX3.

Re-connect cables and reassemble the HX3 body-worn components.

Connecting the Ring Scanner/Imager to the HX3



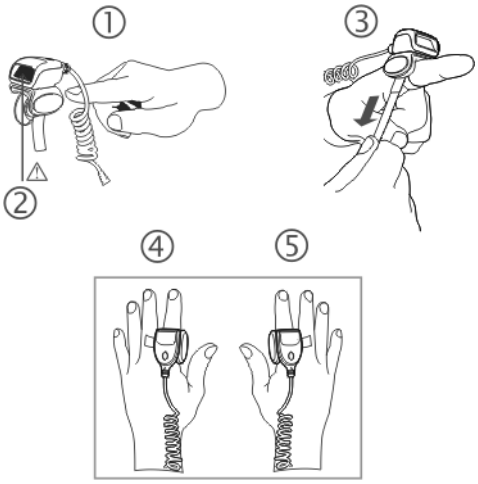
1. Connect
2. Ring on Left Hand
3. Ring on Right Hand
4. Press Down
5. Remove

When you want to switch connectors from left to right, or vice versa, first gently press downward on the Retaining Clip, then pinch and pull the cable connector (not the cable!) straight up and away from the HX3. Do not use a metal object, or extreme force, to remove the cable connector from the HX3.

Re-connect cables and reassemble the HX3 body-worn components.

Attaching the Ring to your Finger

The ring finger loop is located under the ring assembly.



1. Slide finger into opened loop
2. Remove shipping film on scan aperture before first bar code scan
3. Tighten the finger loop strap
4. Ring worn on left hand
5. Ring worn on right hand

Pull gently on the end of the finger loop strap to separate the hook and loop fabric.

Slide your finger into the opened loop under the ring scanner.

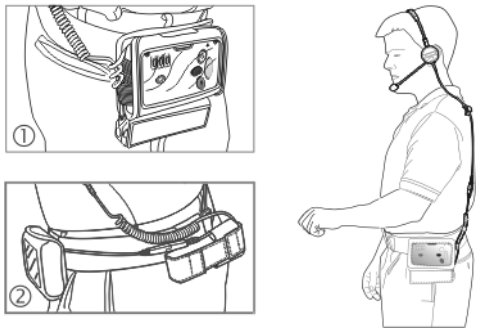
Grasp the end of the finger loop strap and loosen, then tighten, the finger strap until the ring scanner is comfortably snug and the scan aperture is secured in the desired location.

The ring scanner has a built-in quick disconnect designed for occasional safety hazards. It is not intended for frequent, normal removal of the ring scanner from the hand.

Do not touch, push against or brace your finger on the scan aperture at any time.

Assembling the Voice Case

The voice case is a sturdy, lightweight covering for the HX3, tethered battery, and voice accessories. The voice case cannot protect the HX3 from destructive, excessive force or a harsh or wet environment. It is designed to protect the HX3 from dirt, dampness, and minor, trivial bumps.



1. Standard Battery Placement
2. Alternative Battery Placement

1. Slide the belt through the belt loop on the voice case. Do not put the belt on yet.
2. Attach the battery cable, ring scanner, if used, and audio headset to the HX3.
3. Slip the HX3 into the voice case. Be sure the screen and keypad are visible through the clear window of the voice case.
4. Slide the battery cable through the protective loop at the bottom of the voice case. Make sure the tethered cable for the ring accessory is on the outside of the voice case.
5. Slip the battery into the battery sleeve and connect the battery to the battery cable. The battery charge terminals (small metallic circles) should always be covered by the sleeve.
6. Press the hook and loop fabric at the top of the device together.
7. The HX3 in the Voice Case is ready for use.
8. Put the belt on. Adjust the belt and voice case for comfort.
9. Examine the tethers and the hook and loop fabric fastening periodically. If any are loose or unfastened, tighten the tethers and the top fastener before placing the voice case back into service. If the voice case is damaged, it should be removed from service.
10. An HX3 with a voice case does not fit in the desktop cradle. Remove the voice case before placing the HX3 in the desktop cradle.

Setting up the Software on the HX3

Note: Although the HX3 has no display or alphanumeric keypad, HX3 operating system screens can be viewed and parameters manipulated using LXEConnect and ActiveSync on a connected host computer.

1. ActiveSync or Windows Mobile Device Center must be installed on a host computer with a USB port.
2. Connect the assembled HX3 to the host computer using the USB-Client cable.
3. Press the Power key on the HX3. The LEDs begi n to flash. Beeps may be heard from the speaker.
4. Copy LXEConnect setup files from the HX3 to the host computer, if necessary.
5. Launch LXEConnect on the host computer.

The next screen displayed on the host computer is the HX3 Startup page. Use the host computer mouse and keyboard to explore and manipulate control panel settings on the HX3.

If the first screen displayed on the host computer is the HX3 End User Licensing Agreement, click the Accept button to accept the EULA. The HX3 proceeds to start up and the System LEDs begin to flash.

HX3 LEDs

LEDs (Light Emitting Diodes) are grouped together at the top left on the front of the HX3. They are:

System Status LED (located on the right in the group of three LEDs) indicates power management status.

- Wireless Activity LED (located on the left in the group of three LEDs).
- Bluetooth Status LED (located in the middle of the group of three LEDs) indicated Bluetooth client functions.

System Status LED

Blinking Red	Main battery power fail; critical suspend mode
Steady Red	Main battery low. If the main battery is not replaced with a fully charged battery before the internal battery fails, the HX3 is turned Off.
Blinking Green	The HX3 is On and attached to either a battery with a good charge or to an external power source.
Steady Green	The HX3 is booting up.
Off	HX3 is Off (both batteries depleted) or the HX3 is in Suspend mode

Bluetooth Status LED

Blinking Slowly	Bluetooth is paired but not connected to a device.
Blinking Medium	Bluetooth is paired and connected to a device.
Blinking Fast	Bluetooth is discovering Bluetooth devices.
Off	Bluetooth hardware has been turned off or it does not exist in the HX3.

Wireless Activity

Flickering Amber	HX3 is booting up.
Steady Amber	The HX3 is connected to a wireless network.
Off	The HX3 has not connected to a wireless network.

Set Date and Time Zone

Click the **Start > Settings > Control Panel > Date/Time** icon.

Set Date, Time, Time Zone, and assign a Daylight Savings location on the HX3 after a warm boot or anytime.

There is very little functional change from standard desktop PC Date/Time Properties options. Adjust the settings and click the OK button or the Apply button to save changes to the registry. Any changes take effect immediately.

Double-clicking the time displayed in the Taskbar causes the Date/Time Properties screen to appear.

Set Speaker Volume

The speaker is on the front, above the white key.

Speaker volume can be adjusted to a comfortable level for the listener by using the keypad or by changing parameters in the Volume & Sounds control panel.

Using the Keypad

*Note: Volume & Sounds (in **Settings > Control Panel**) must be enabled before the following key sequences can adjust the volume.*

Note: The volume is increased or decreased one step each time the volume key sequence is pressed.

Note: To adjust speaker volume use the Blue+White keys and Blue+Green keys to adjust volume until the speaker volume is satisfactory.

Volume control using a keypad key press has six volume settings that match those supported by the Volume and Sounds Control panel. Volume does not “roll-over” from minimum to maximum or from maximum to minimum. Continuously holding down the up or down arrow keys does not cause an automatic repeat of the up (or down) arrow key.

Using the Control Panel

Note: When the HX3 is connected via ActiveSync to a PC running LXEConnect, the Volume and Sounds option in the Control Panel can be used to adjust volume.

Tap **Start > Settings > Control Panel > Volume & Sounds > Volume** tab. Change the volume setting and tap OK to save the change.

You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft.

As the volume scrollbar is moved between Loud and Soft, the HX3 emits a tone each time the volume increases or decreases.

Using the Input Panel / Virtual Keyboard

The virtual keyboard is always available when needed e.g., text entry.

Place the cursor in the text entry field and, using the stylus:

- Tap the Shift key to type one capital letter.
- Tap the CAPS key to type all capital letters.
- Tap the áü key to access symbols.

Some applications do not automatically display the Input Panel. In this case, do the following to use the Input Panel:

- Move the cursor into the text entry field when you want to enter data using the Input Panel.
- When finished entering data, tap the icon in the Taskbar again.

Connecting Bluetooth Devices

Before connecting to Bluetooth Devices:

- The system administrator has discovered, paired, connected and disconnected (using LXEZ Pairing Control Panel) Bluetooth devices for each HX3.
- The system administrator has enabled and disabled LXEZ Pairing parameters for the HX3.
- The system administrator has also assigned a Computer Friendly Name using LXEZ Pairing Control Panel for the HX3.

To connect Bluetooth devices, the HX3 should be as close as possible and in direct line of sight (distances up to 32.8 feet or 10 meters) with the targeted Bluetooth device during the discovery and pairing process.

If the devices are in Suspend, tap the power key to wake the HX3. Using the correct procedure, wake the targeted Bluetooth device if necessary.

There may be audible or visual signals as both devices discover and pair with each other.

Taskbar Connection Indicator

	HX3 is connected to one or more of the targeted Bluetooth device(s).
	HX3 is not connected to any Bluetooth device. HX3 is ready to connect with any Bluetooth device. HX3 is out of range of all paired Bluetooth device(s). Connection is inactive.

LED Connection Indicator

When the Bluetooth LED on the HX3 is off, Bluetooth hardware has been turned off or it does not exist in the HX3.

When the Bluetooth LED on the HX3 is on:

- the HX3 is paired with another Bluetooth device but is out of range or not connected, or
- is paired and connected to another Bluetooth device, or
- is discovering other Bluetooth devices.

The Bluetooth LED

- Blinks slowly (Bluetooth LED is on for one second, off for five seconds) when it is idle.
- Blinks quickly (Bluetooth LED is on for 1/4 second, off for 2 seconds when the HX3 is discovering other Bluetooth devices.
- And blinks normally (Bluetooth LED is on for 1/2 second, off for 1/2 second) when it is connected.
- There may be audible or visual signals from paired devices as they move back into range and re-connect with the Bluetooth hardware in the HX3.

Reboot

When the HX3 desktop is displayed on the host computer or an application begins, the power up (or reboot) sequence is complete. The HX3 must be connected to a host computer and LXEConnect must be active before proceeding to warm boot or cold boot. Verify the HX3 has a known good power source, either a fully charged battery or docked in a powered desktop cradle.

Warm Boot

Start > Run

A warm boot function does not affect the HX3 operating system, but data and programs in RAM are cleared, and registry changes, if any, are saved. Network, ActiveSync and Bluetooth connections will need to be re-established.

Tap **Start > Run** and type WARMBOOT.EXE or WARMBOOT. This command is not case sensitive. Tap the **OK** button. This process takes less than 15 seconds. Temporary data not saved is lost.

Warm boot terminates the host computer ActiveSync connection. The host computer connection must be re-established after the HX3 boots.

There may be slight delays while the wireless client connects to the network, re-authorization for voice-enabled applications completes, Wavelink Avalanche management of the HX3 startup completes, or Bluetooth relationships establish or re-establish.

Cold Boot

Start > Run

The cold boot function reboots the HX3, erases all registry data and user-specified settings. The factory default settings are restored when the HX3 powers on again.

Click **Start > Run** and type COLDBOOT.EXE or COLDBOOT. This command is not case-sensitive. Click the **OK** button.

Cold boot terminates the host computer connection. The host computer connection must be re-established after the HX3 cold boots.

Because of the extreme nature of cold boot, use this command only as an emergency or when instructed to do so as part of a specific HX3 procedure.

Startup Help

Contact Customer Support (page 14-1) if you need more help.

Issue:

HX3 seems to lockup as soon as it is rebooted.

Solution:

There may be slight delays while the wireless client connects to the network, authorization for voice-enabled applications complete, Wavelink Avalanche management of the HX3 startup completes and Bluetooth relationships establish or re-establish. When an application begins, the HX3 is ready for use.

Issue:

New HX3 main batteries don't last more than a few hours.

Solution:

New batteries must be fully charged prior to first use. Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember – the HX3 is always ‘on’ even when in the Suspend state and draws battery power at all times.

3

Hardware Configuration

System Hardware

802.11b/g and a/b/g Wireless Client

The HX3 has an 802.11x network card that supports diversity with two internal antennas. The CPU board does not allow hot swapping the network card. Adjusting power management on the network card is set to static dynamic control.

WEP, WPA and LEAP are supported.

Central Processing Unit

The CPU is a 400MHz Intel XScale PXA255 CPU. The operating system is Microsoft® Windows® CE 5. The OS image is stored on an internal SD flash card and is loaded into DRAM for execution.

XScale turbo mode switching is supported and turned on by default.

The HX3 supports the following I/O components of the core logic:

- One SD card slot, inaccessible to the end-user.
- One TTL serial port designed to interface with the ring scanner only.
- One RS232 serial port accessible via the cradle.
- USB master accessible via the cradle.
- USB client accessible via the cradle.

System Memory

The 400MHz CPU configuration supports 128MB SDRAM, 128MB SD card. SD card location is inaccessible to the end user.

The system optimizes for the amount of SDRAM available. The operating system executes out of RAM.

Internal flash is used for boot loader code and system low-level diagnostics code. Bootloader code is validated at system startup. The UUID required by CE 5.0 is stored in the boot flash. A second copy of the bootloader code is stored on the internal SD Flash drive, so that if a damaged bootloader is detected, it may be re-flashed correctly.

Internal SD Memory Card

The HX3 has one SD card interface for storage of operating system and program code, as well as persistent storage. The SD slot is inaccessible and ships with a qualified 128MB (optional 512MB) SD Flash card.

The internal SD flash card supports a FAT file system, via a special device driver, and appears to the OS as a folder. This allows the contents to be manipulated via the standard Windows CE interface. Operating system files are hidden on this drive with a terminal unique identifier in the internal flash, to prevent them being accidentally erased by a user. In addition, the registry hive files are stored on this device. The amount of Flash memory available for customer use is the original SD flash card size less 40MB.

Power Supply

The HX3 uses two batteries for operation. A Lithium-Ion (Li-Ion) battery supplies power to the HX3 only when tethered to the HX3. The main battery is either the 2000 mAh (Standard) or the 4000 mAh (Extended) battery. Only one main battery can be tethered to the HX3 at a time. The batteries can be hot-swapped after the HX3 is placed in Suspend mode.

The internal backup battery is a 50 mAh Nickel Cadmium (NiCad) battery. The backup battery is recharged indirectly by the HX3 with a tethered battery. Recharging maintains the backup battery near full charge at all times. When the backup battery is fully drained, it may take up to 5 hours to recharge. The capability to discharge the backup battery is provided (**Start > Settings > Control Panel > Battery**) to allow the user to condition the backup battery in order to recover full battery capacity. The backup battery must be replaced by qualified service personnel. The backup battery has a minimum 2 year service life.

When the HX3 is docked in a HX2 labeled powered desktop cradle, the HX3 receives USB/serial signals through the cradle connector on the bottom of the HX3 and the cradle connector in the HX2 docking bay. The HX3 must be firmly seated in the docking bay before USB/serial communication can occur. An extra standard or extended Li-Ion battery pack can be recharged in the powered cradle while one of the batteries is tethered to, and powering, the HX3. The standard battery is fully recharged in a powered cradle in 4 hours. The extended battery is fully recharged in 8 hours.

Docked HX3 -- An uninterrupted external power source (wall AC/DC adapter connected to the HX2 cradle) transfers signals from the USB ports in the front of the cradle and the serial port on the back of the cradle, to the HX3. HX3 frequent connection to a fully charged tethered battery, is recommended to maintain backup battery charge status, as the backup battery cannot be recharged by a dead or missing tethered battery.

The HX2 labeled Battery Charger is designed to simultaneously charge up to six standard Rechargeable Lithium Ion Battery Packs in less than four hours, depending upon battery pack temperature and ambient conditions. The Extended battery packs require less than 8 hours. The Battery Charger can charge up to five Standard and Extended batteries when they are not tethered to the HX3.

Bluetooth

The HX3 contains Bluetooth version 2.0 with Enhanced Data Rate (EDR) up to 3.0 Mbit/s over the air. Bluetooth device connection (or pairing) can occur at distances up to 32.8 ft (10 meters) Line of Sight. The wireless client retains wireless connectivity while Bluetooth is active.

The user will not be able to select PIN authentication or encryption on connections to from the HX3. However, the HX3 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the HX3 displays a prompt for the PIN or passcode. Maximum encryption is 128 bit. Encryption is based on the length of the user's passcode.

The Bluetooth client can simultaneously connect to one Bluetooth scanner and one Bluetooth printer. Up to four Bluetooth devices can be paired and managed using a control panel (**Start > Settings > Control Panel > Bluetooth**).

Blue LED	Blinking slowly	Bluetooth is active but not connected to a device.
Blue LED	Blinking medium	Bluetooth is paired and connected to a device.
Blue LED	Blinking fast	Bluetooth is discovering other Bluetooth devices.
Blue LED	Unlit	Bluetooth hardware has been turned off or does not exist in the HX3.

Bar code data captured by the Bluetooth scanner is manipulated by the settings in the Scanner Properties control panel.

Multiple beeps may be heard during a bar code scan using a mobile Bluetooth scanner; beeps from the mobile Bluetooth scanner as the bar code data is accepted/rejected, and other beeps from the HX3 during final bar code data manipulation.

Input/Output Connectors

The HX3 has three I/O connectors. Two connectors are located next to each other on the back of the mobile device. Each of the two connectors (one for left-handed users and the other for right handed users) interfaces with peripherals such as a Laser Ring Scanner, an Imager Ring Scanner, an audio headset and a tethered battery.

Connector 1 and Connector 2 are located on the back of HX3 and each connector can accommodate a:

- Tethered Laser or Imager Scanner
- Tethered Headset/Microphone and HX3 Battery
- Tethered Battery

Connector 3 is located on the bottom of HX3 and can accommodate:

- Cradle
- Cradle Power Input
- USB Keyboard and mouse through cradle

The third I/O connector is used when docking the HX3 in a cradle. The cradle has RS232, USB Client, unpowered USB Host and Power connections. The power connection on the cradle supplies power to the battery charging bays. All communication is managed by the cradle.

Audio Support

Speaker

The internal speaker supplies audible verification signals normally used by the Windows CE operating system. The speaker is located on the front of the HX3, above the [2] key. The mobile device emits a Sound Pressure Level (loudness) of at least 102 dB measured as follows:

Frequency: 2650 + 100 Hz

Distance: 10 cm on axis in front of Speaker opening in front of unit.

- Duration : Continuous 2650 Hz tone.
- The default is 1 beep for a good scan and 2 beeps for a bad scan.
- Volume Control
- Volume control is managed by a Windows CE control panel applet, an API and key sequences. To adjust speaker volume use the Blue+White (Volume Up) and Blue+Green (Volume Down) buttons.

Volume control is covered in greater detail later in this guide.

Voice

All Microsoft-supplied audio codecs are included in the OS image. The hardware codecs, the input and output analog voice circuitry and the system design are designed to support voice applications using a headset connected to the “Tethered Headset/Microphone and HX3 Battery” accessory cable.

4

Power Modes and Batteries

Modes

The HX3 has three power modes; On, Suspend and Off.

Primary Events Listing

- Any key on the keypad
- COM1 activity
- Docked in powered cradle
- Power button tap
- Bluetooth device reconnect / disconnect message
- Ring scanner activity

On Mode

After a new HX3 has been received, a charged battery tethered, and the Power key tapped, the HX3 is always On until both batteries are drained completely of power.

When the tethered battery and backup battery are drained completely, the unit is in the Off mode. The unit transitions from the Off mode to the On mode when a charged battery is attached to the tether or external power is applied (for example, by docking the HX3 in a powered cradle) and the HX3 Power key is pressed.

Suspend Mode

The Suspend mode is entered when the unit is inactive for a predetermined period of time or the user taps the Power key.

HX3 Suspend timers are set using **Start > Settings > Control Panel > Power > Schemes** tab.

Wake up Events - all configurable via a Power Management API call:

- Any key on the keypad
- Scan button on ring scanner or ring imager pressed
- Docked in a powered cradle
- Power button tap

When the unit wakes up, the Power Off timers begin the countdown again. When any one of the above events occurs prior to the Power Off timer expiring, the timer starts the countdown again.

The HX3 should be placed in Suspend Mode before hotswapping the main battery.

Hotswapping the Ring Scanner does not require placing the HX3 in Suspend Mode.

Off Mode

The unit is in Off Mode when the tethered battery and the backup battery are depleted. Connect a fully charged main battery and press the Power key to turn the HX3 On.

Batteries

The HX3 is designed to work with a Lithium-Ion (Li-ion) tethered battery. Under normal conditions it should last approximately eight to ten hours before requiring a recharge. The more you use the ring scanner or the wireless transmitter, the shorter the time required between battery recharges.

A suspended HX3 maintains the date and time for a minimum of two days while tethered to a battery that has reached the Low Warning point and a fully charged backup battery. The HX3 retains data, during a battery hot swap, for at least 5 minutes.

New battery packs must be charged prior to use. The Standard batteries require less than four hours and the Extended batteries require less than 8 hours.

Checking Battery Status

This option requires a host computer ActiveSync connection and LXEConnect.

Click the **Start > Settings > Control Panel > Power > Battery** tab. Battery level, power status and charge remaining is displayed. Turbo setting is enabled/disabled using this applet.

Battery power drain increases substantially in Turbo mode.

Status LED and the Batteries

When the Status LED is ...	The HX3 Status is ...	
Green - Steady	Booting	The HX3 is booting.
Green - Blinking	On	HX3 is attached to a charged Main Battery or to an external power source.
Red - Steady	Main Battery Low	Low Battery Warning. If the main battery is not replaced with a fully charged battery before the main battery fails, the HX3 is turned Off.
Red - Blinking	Main Battery Power Fail	Replace the main battery with a fully charged main battery.
Off	Off	The main battery is depleted, the HX3 is not attached to a power source and the backup battery is also depleted.

Low Battery Warning

It is recommended that the main battery pack be removed and replaced when its energy depletes. When the main battery Low Battery Warning appears (the Status LED remains a steady red) perform an orderly shut down, minimizing the operation of any installed devices and insuring any information is saved that should be saved.

Once you receive the main battery Low Battery Warning, you have approximately 5 minutes to perform an orderly shutdown and replace the main battery pack before the device powers off. The Low Battery Warning will transition the mobile device to Suspend before the device powers off.

Main Battery Pack

The main battery pack has a rugged plastic enclosure that is designed to withstand the ordinary rigors of an industrial environment. Exercise care when transporting the battery pack making sure it does not come in contact with excessive heat or any power source other than the HX2 labeled Battery Charger, HX2 labeled Desktop Cradle or the HX3 unit.

Whenever possible, protect the battery charging terminals (five small round circles) by keeping them covered by the battery sleeve fabric. The battery pack is resistant to impact damage.

Under normal conditions a properly tethered Standard battery should last a minimum of approximately eight hours before requiring a recharge, the Extended battery a minimum of approximately 16 hours.

Battery Hotswapping

Important: When the backup battery power is Low or Very Low (**Start > Settings > Control Panel > Power > Battery** tab) dock the HX3 in a powered docking cradle before replacing the battery pack.

When the main battery power level is low, the HX3 will signal the user with the low battery warning indicator (the Status LED remains a steady red) that continues until the main battery is replaced, the battery completely depletes, or external power is applied to the HX3 using a powered cradle.

You can replace the main battery by first placing the device in Suspend Mode then removing the discharged main battery and tethering a charged main battery within a five minute time limit (or before the backup battery depletes).

Placing the HX3 in Suspend terminates the ActiveSync connection, if one is established. The ActiveSync connection must be re-established after the HX3 exits Suspend.

When the main battery is disconnected the device enters Critical Suspend state, the HX3 remains in Suspend mode, the display is turned off and the backup battery continues to power the unit for at least five minutes. Though data is retained, the HX3 cannot be used until a charged main battery pack is connected. After tethering the full battery, press the Power key.

Full operational recovery from Suspend can take several seconds while the wireless client connects to the network, authorization for voice-enabled applications complete, Wavelink Avalanche management of the HX3 startup completes, and Bluetooth relationships establish or reestablish.

If the backup battery depletes before a fully charged main battery can be inserted, the HX3 will turn Off.

Backup Battery

The HX3 has a backup battery that is designed to provide limited-duration electrical power in the event of main battery failure. The backup battery is a 50 mAh Nickel Cadmium (NiCd) battery that is factory installed in the unit. The energy needed to maintain the backup battery near full charge at all times comes from the HX3 main battery.

It takes several hours of operation before the backup battery is capable of supporting the operation of the mobile device. The duration of backup battery life is dependent upon operation of the HX3, its features and any operating applications.

The backup battery has a minimum service life of two years. The backup battery is not user-serviceable.

The backup battery can be discharged, recharged and conditioned using a CE Control Panel applet. Tap **Start > Settings > Control Panel > Battery** then tap the **Discharge** button.

Handling Batteries Safely

Never dispose of a battery in a fire. This may cause an explosion.

- Do not replace individual cells in a battery pack.
- Do not attempt to pry open the battery pack shell.
- Be careful when handling any battery. If a battery is broken or shows signs of leakage do not attempt to charge it. Dispose of it using proper procedures.
- Nickel-based cells contain a chemical solution which burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention.
- NiCd and Li-Ion batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a battery in a pocket or case with keys, coins, or other metal objects.

5

Software Configuration

Using ActiveSync

Before any software configuration can occur, the HX3 must be connected to a host computer with a USB port. The HX3 does not have a touch screen. Because of this and the limited keypad, it is necessary to configure the HX3 using ActiveSync and LXEConnect.

Note: The HX3 does not have a touch screen. If the host computer has a touch screen, instructions using "tap" and "stylus" instead of "click" and "mouse" apply.

Note: Once a relationship (partnership) has been established with ActiveSync Connect (on a host computer), ActiveSync will synchronize using the wireless link, serial port, or USB on the HX3.

Note: ActiveSync serial connection requires a powered desktop cradle.

Requirement : ActiveSync (version 4.5 or higher for Windows XP host computers) must be resident on the host computer. Windows Mobile Device Center (version 6.1 or higher) is required for a Windows Vista or greater host computer. ActiveSync and Windows Mobile Device Center for the PC is available from the Microsoft website. Follow Microsoft's instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your host computer.

Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or greater operating system on your host computer, replace ActiveSync with Windows Mobile Device Center.

Using Microsoft ActiveSync, you can synchronize information on your host computer with the HX3 and vice versa. Synchronization compares the data on your HX3 with your host computer and updates both with the most recent data.

For example, you can:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and host computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your host computer or only when you choose the synchronize command.

By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your host computer and your device.

When installation of ActiveSync is complete on your host computer, the ActiveSync Setup Wizard begins and starts the following processes:

- connect your mobile device to your host computer,
- set up a partnership so you can synchronize information between your mobile device and your host computer, and
- customize your synchronization settings.

Because ActiveSync is already installed on your mobile device, your first synchronization process begins automatically when you finish setting up your host computer in the ActiveSync wizard. For more information about using ActiveSync on your host computer, open ActiveSync, then open ActiveSync Help.

Initial Setup

The initial setup of ActiveSync must be made via a USB.This is the only connection type supported on the HX3.

Partnerships can only be created using USB cable connection.

Connect via USB

The default connection type is USB Client

IMPORTANT: This setting must not be changed on the HX3!

To change the connection type or to verify it is set to USB, select **Start > Settings > Control Panel > PC Connection**.

Tap the Change button. From the popup list, choose **USB Client**.

This will set up the HX3 to use the USB port. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel. If desired, any control panel windows may be closed.

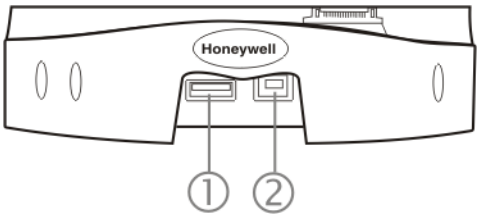
IMPORTANT – DO NOT PUT THE HX3 INTO SUSPEND WHILE CONNECTED VIA USB. The device will be unable to connect to the host PC when it resumes operation.

Connect the correct cable to the PC (the host) and the mobile device (the client) as detailed below. USB will start automatically when the USB cable is connected, not requiring you to select “Connect” from the start menu.

Cable for USB ActiveSync Connection

When a cradle is used:

HX2312DSKCRDL or HX2313DSKCRDL - HX2-labeled desktop cradle



Use with standard USB cable with type A plug for PC/Laptop USB port and type B plug for HX3 cradle USB type B client port.

- Plug the type B end of the standard USB cable plug into the USB type B port on the desktop cradle (port #2).
- The USB type A connector on the standard cable connects to a USB port on a PC or laptop.
- The USB client (port #1) connector on the cradle does not need to be connected.

If a cradle is not used:

HX2001CABLE - ActiveSync cable for HX3 when not in the desk dock. Cable connects directly to the HX3 and the other end connects to host computer USB port.

- Insert the HX3 cable end into the cradle connector on the bottom of the HX3.
- The USB type A connector on the cable connects to a USB port on a PC or laptop.

Note: The ActiveSync cable for the HX3 does not appear to fit tightly with the cradle connector, but at an angle. This is normal.

Synchronizing from the HX3

To initiate synchronization from your host computer, tap **Start > Programs > Communication > ActiveSync** to begin the process.

Tap **Sync** to connect and synchronize. View synchronization status.

Tap **Tools** to synchronize or change synchronization settings. View connection status.

Tap **Stop** to stop synchronization.

Tap **Start > Help** for context-sensitive help.

Explore

From the ActiveSync Dialog on the host computer, tap the Explore button, which allows you to explore the HX3 on the host computer, with some limitations. You can copy files to or from the HX3 by drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows folder on the HX3. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows image. This, however, includes most of the files in the \Windows folder).

Backup Data Files using ActiveSync

Use the following information to backup data files from the HX3 to a host computer using the appropriate cables and Microsoft’s ActiveSync.

Note: A partnership between the HX3 and ActiveSync on the host computer must be established before backup can occur.

Note: USB Transfer

- A host computer with an available USB port and a desktop cradle with a USB port. The host computer must be running Windows XP or greater.
- Use the specific USB cable as listed in Connect Via USB.

Connect

Connect the USB cable to the host computer and the HX3 in the desktop cradle (the client). Select Connect from the Start Menu on the mobile device (**Start > Programs > Communications > Connect**).

Note: USB connection will start automatically (this is the default) when the cable is connected, not requiring you to select Connect from the Start menu.

Disconnect

- Disconnect the cable from the mobile device or desktop cradle.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

IMPORTANT – Do not put the mobile device into Suspend while connected via USB. The device will be unable to connect to the host computer when it resumes operation.

Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a client and a host computer. A partnership is defined by two objects – a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership between a unique client can be established to two hosts.

When the mobile device is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host computer retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host computer if they have the same name. (**Control Panel > System > Device Name**)

If the cold booted mobile device tries to reestablish the partnership with the same host PC, a new random number is generated for the mobile device and ActiveSync will insist the unique name of the mobile device be changed. If the mobile device is associated with a second host, changing the name will destroy that partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

ActiveSync Help

Issue:

ActiveSync on the host says that a device is trying to connect, but it cannot identify it

Solution:

One or more control lines are not connected. This is usually a cable problem.

If the HX3 is connected to a host computer by a cable, disconnect the cable from the HX3 and reconnect it again.

Issue:

ActiveSync indicator on the host (disc in the toolbar tray) turns green and spins as soon as you connect the cable, before tapping the Connect icon (or REPLLOG.EXE in the Windows directory).

Solution:

One or more control lines are tied together incorrectly. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

Issue:

ActiveSync indicator on the host turns green and spins, but connection never occurs.

Solution:

Incorrect or broken data lines in cable.

Issue:

ActiveSync indicator on the host remains gray

Solution:

Solution 1: ActiveSync icon on the host computer does not turn green after connecting USB cable from HX3.

Disconnect HX3 USB cable from host computer.

1. Suspend/Resume or Restart the HX3.
2. Reconnect USB cable from HX3 to host computer.

Solution 2: The host doesn't know you are trying to connect. May mean a bad cable. Try the connection again, with a known good cable.

Configuring the HX3 with LXEConnect

LXEConnect allows a user to view the HX3 screen remotely on a host computer using an ActiveSync connection:

Requirement : ActiveSync (version 4.5 or higher for Windows XP host computers) must be resident on the host computer. Windows Mobile Device Center (version 6.1 or higher) is required for a Windows Vista or greater host computer. ActiveSync and Windows Mobile Device Center for the PC is available from the Microsoft website. Follow Microsoft's instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your host computer.

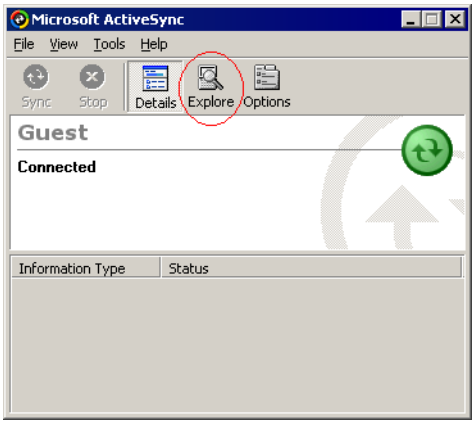
Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or greater operating system on your host computer, replace ActiveSync with Windows Mobile Device Center.

ActiveSync is already installed on the HX3. The HX3 is preconfigured to establish a USB ActiveSync connection to a PC when the proper cable is attached to the HX3 and the PC.

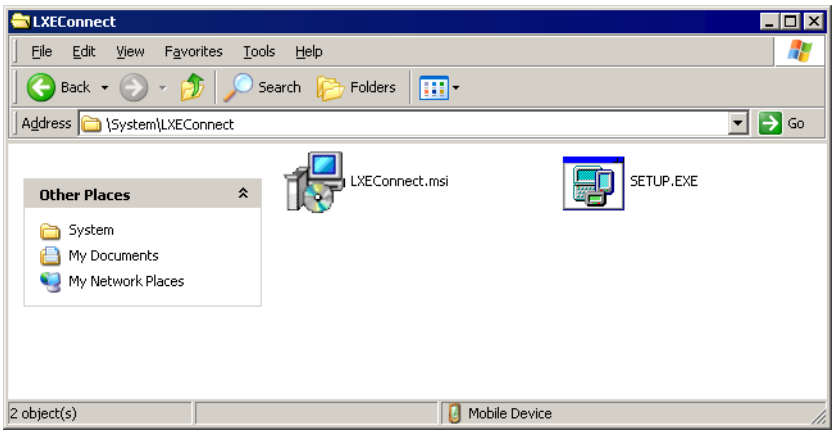
If the HX3 uses a serial port for ActiveSync, it will be necessary to configure the HX3 to use the serial port. Complete details on the proper cables and port configuration are included in Initial Setup (page 5-1).

Install LXEConnect

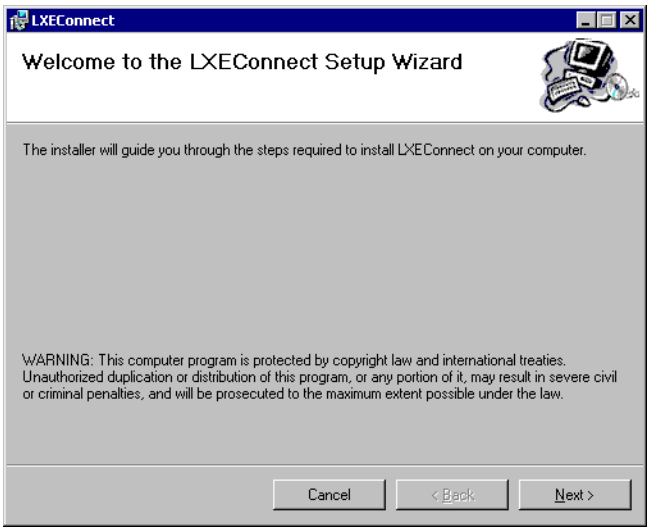
1. Install Microsoft ActiveSync on a host computer with a USB port. For details, see Initial Setup (page 5-1).
2. Power up the HX3.
3. Connect the HX3 to the host computer using the proper connection cable. Once connected, the ActiveSync dialog box appears. If using the USB connection, the ActiveSync connection is automatically established.
4. Select "No" for partnership when prompted. Dismiss any ActiveSync dialog boxes warning a partnership is not set up. It is not necessary to establish a partnership to use LXEConnect. However, if a partnership is desired for other reasons, one may be established now. More details on partnerships are included in ActiveSync Help.
5. When the ActiveSync screen appears, select Explore.



6. An explorer window is displayed for the HX3. Contact Customer Support (page 14-1) for the necessary files if this folder is not present .



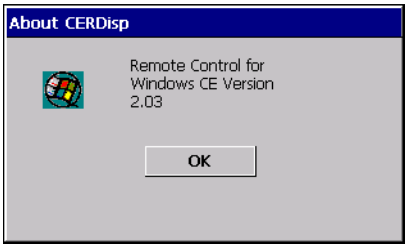
7. Select and copy the LXEConnect.msi and Setup.exe files from the HX3 to the host computer. Note the location chosen for the files.
8. Close the ActiveSync explorer dialog box. Do not disconnect the HX3 ActiveSync connection.
9. Execute the setup.exe file that was copied to the host computer. This setup program installs the LXEConnect utility.



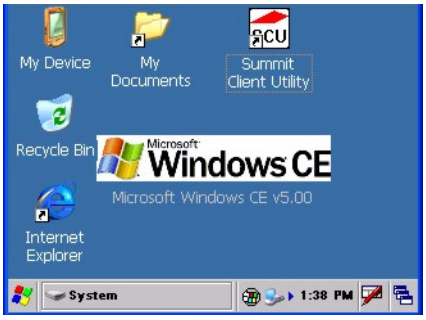
10. Follow the on screen installation prompts. The default installation directory is C:\Program Files\LXE\LXEConnect.
11. When the installation is complete, create a host computer desktop shortcut to the following file: C:\Program Files\LXE\LXEConnect\LXEConnect.exe. If a different directory was selected during installation, substitute the appropriate directory.
12. LXEConnect is now installed on the host computer and ready to use.

Using LXEConnect

1. If an ActiveSync connection has not been established, connect the HX3 to the host computer. Details on ActiveSync are included in the previous section.
2. Double-click the LXEConnect icon that was created on the host computer desktop.
3. LXEConnect launches.



4. Click the OK button to dismiss the About CERDisp dialog box on the desktop by clicking the OK button in the LXE-Connect window on the host computer desktop. The dialog box automatically times out and disappears after approximately 20 seconds.



5. The HX3 can now be configured from the host computer LXEConnect window. Input from the PC's mouse and keyboard are recognized as if they were attached to the HX3.
6. When the remote session is completed, terminate the LXEConnect program by selecting **File > Exit** or clicking on the X in the upper right hand corner to close the application, then disconnect the ActiveSync cable.

Note: After using LXEConnect, the HX3 cannot go into Suspend mode until after a warmboot. If using Power Management on a HX3, always warmboot the HX3 when finished using LXEConnect.

Operating System and Software Load

There are several different aspects to the setup, configuration and operation of the HX3. Many of the setup and configuration settings are dependent upon the optional features such as hardware and software installed on the unit. The examples found in this section are to be used as examples only, the configuration of your specific HX3 computer may vary. The following sections provide a general reference for the configuration of the HX3 and some of its optional features.

Note: HX3 applications, operating system settings and control panels must be viewed and edited / updated using LXEConnect and ActiveSync on a host computer cabled to the HX3.

Windows CE Operating System

Note: For general use instruction, refer to commercially available Windows CE user's guides or the Windows CE on-line Help application installed with the HX3.

Your HX3 operating system is Microsoft® Windows® CE 5. The HX3 operating system revision is displayed on the Desktop. This is the factory default setting for the Desktop Display Background.

This segment assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the HX3 and its Windows CE environment.

General Windows CE Keyboard Shortcuts

Use the keyboard shortcuts in the chart below to navigate with the HX3 keyboard displayed in the LXEConnect window on a host computer. These are standard keyboard shortcuts for Windows CE applications.

Press these keys …	To …
CTRL + C	Copy
CTRL + X	Cut
CTRL + V	Paste
CTRL + Z	Undo
DELETE	Delete
SHIFT with any of the arrow keys	Select more than one item in a window or on the desktop, or select text within a document.
CTRL+A	Select all.
ALT+ESC	Cycle through items in the order they were opened.
CTRL+ESC	Display the Start menu.
ALT+Underlined letter in a menu name	Display the corresponding menu.
Underlined letter in a command name on an open menu	Carry out the corresponding command.
ESC	Cancel the current task.

Reboot

Two reboot sequences are available; Warmboot and Coldboot.

Warmboot

A warmboot reboots the computer without erasing any registry data. However, any applications installed to RAM are lost, as is all data in RAM. This occurs because the operating system is stored on the flash drive, but must be loaded into RAM to run.

All registry configurations are automatically preserved. Any applications stored as .CAB files in the System folder and configured in the Registry to persist are reinstalled on boot up by the Launch utility.

Coldboot

A coldboot reboots the computer, erases all registry data and returns the computer to factory default settings. In order to be preserved, applications and data must be stored in the System folder. Registry information is not preserved. Only factory default applications and drivers stored as .CAB files in the System folder are loaded by Launch.

A cold boot is initiated by running the Coldboot application in the Windows folder. This application automatically cold boots the HX3, erasing any customer applied registry changes and returning the HX3 to its factory settings.

Clearing Persistent Storage / Reset to Default Settings

The coldboot utility sets all registry settings back to factory defaults. No other clearing is available or necessary.

Folders Copied at Startup

The following folders are copied on startup:

System\Desktop	copied to	Windows\Desktop
System\Favorites	copied to	Windows\Favorites
System\Fonts	copied to	Windows\Fonts
System\Help	copied to	Windows\Help
System\Programs	copied to	Windows\Programs
AppMgr	copied to	Windows\AppMgr
Recent	copied to	Windows\Recent

This function copies only the folder contents, no sub-folders.

The Windows\Startup folder is not copied on startup because copying this folder has no effect on the system or an incorrect effect.:

Files in the Windows\Startup folder are executed, but only from System\Startup. Windows\Startup is parsed too early in the boot process so it has no effect.

Executables in System\Startup must be the actual executable, not a shortcut, because shortcuts are not parsed by Launch.

Saving Changes to the Registry

The HX3 saves the registry when you:

Tap **Start > Run t**hen type Warmboot. Tap **OK**.

- Perform a Suspend / Resume function (by pressing the Pwr key and then pressing it again).

The registry save process takes 0 – 3 seconds. If nothing has been changed, nothing is saved (e.g., 0 seconds)

The registry is automatically saved every 20 minutes. It is also saved every tenth time the registry settings are changed. Registry settings are changed when control panel applet (e.g., Date/Time) parameters are changed by the user and a warm boot was not performed afterward.

When you tap **Start > Run** then type **Coldboot** and tap the **OK** button, factory default registry settings are loaded during coldboot. All customized changes and settings are lost.

Software Load

The software loaded on the HX3 consists of the Windows OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

- Full Operating System License: Includes all operating system components, including Microsoft® Windows® CE 5 kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touch screen input, window management, and common controls.
- Network and Device Drivers
- Bluetooth (Option)

Software Applications

The following applications are included:

- WordPad
- Scan Wedge (bar code result manipulation)
- ActiveSync
- Internet Explorer

Bluetooth (Option)

Start > Settings > Control Panel > Bluetooth

Only installed on a Bluetooth equipped HX3. The System Administrator can Discover and Pair targeted Bluetooth devices for each HX3. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly name for each HX3.

The Bluetooth control panel can also be accessed by doubletapping the Bluetooth icon in the taskbar or on the desktop.

Avalanche

The Wavelink Avalanche Enabler installation file is loaded on the HX3; however, the device is not configured to launch the installation file automatically. The installation application must be run manually the first time Avalanche is used. Following installation, the Wavelink Avalanche Enabler will be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

Software Development

See Also: *CE API Programming Guide*

The CE API Programming Guide documents HX3-specific API calls. It is intended as an addition to Microsoft Windows CE API documentation.

A Software Developers Kit (SDK) and additional information about software development can be found on the Technical Support Portal. Contact Customer Support (page 14-1) for more information or to access the portal.

Access Files on the Flash Card

Click the My Device icon on the Desktop then click the System icon.

A flash card is used for permanent storage of the HX3 drivers, CAB files and utilities. It is also used for registry content back up.

CAB files, when executed, are not deleted.

Note: Always perform a warm reset (Start / Run / Warmboot) when exchanging one flash card for another.

HX3 Utilities

The following files are pre-loaded.

LAUNCH.EXE

Launch works in coordination with registry settings to allow drivers or applications to be loaded automatically into DRAM at system startup. Registry settings control what gets launched; see the App Note for information on these settings. For examples, you can look at the registry key

HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist

Launch will execute .CAB files, .BAT files, or .EXE files.

App Note

All applications to be installed into persistent memory must be in the form of Windows CE CAB files. These CAB files exist as separate files from the main installation image, and are copied to the CE device using ActiveSync, or using a Compact Flash ATA card. The CAB files are copied from ATA or using ActiveSync Explore into the folder System, which is the persistent storage virtual drive. Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup.

The registry information needed is under the key HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist, as follows. The main subkey is any text, and is a description of the file. Then 3 mandatory values are added:

- FileName is the name of the CAB file, with the path (usually \System).
- Installed is a DWORD value of 0, which changes to 1 once auto-launch installs the file.
- FileCheck is the name of a file to look for to determine if the CAB file is installed. This will be the name of one of the files (with path) installed by the CAB file. Since the CAB file installs into DRAM, when memory is lost this file is lost, and the CAB file must be reinstalled.

There are three optional fields that may be added:

1. Order is used to force a sequence of events. Order=0 is first, and Order=99 is last. Two items which have the same order will be installed in the same pass, but not in a predictable sequence.

2. Delay is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to 0 if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.

3. PCMCIA is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the "Unidentified PCMCIA Slot" dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the PCMCIA field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of 0 means the slot is not powered on. The default values for the default radio drivers (listed below) is 1, meaning one second elapses between the CAB file loading and the slot powering up.

The auto-launch process proceeds as follows:

- The launch utility opens the registry database and reads the list of CAB files to auto-launch.
- First it looks for FileName to see if the CAB file is present. If not, the registry entry is ignored. If it is present, and the Installed flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation), and runs the Microsoft utility WCELOAD to install it.
- If the Installed flag is set, auto-launch looks for the FileCheck file. If it is present, the CAB file is installed, and that registry entry is complete. If the FileCheck file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file.
- Then, the whole process repeats for the next entry in the registry, until all registry entries are analyzed.
- To force execution every time (for example, for AUTOEXEC.BAT), use a FileCheck of "dummy", which will never be found, forcing the item to execute.
- For persist keys specifying .EXE or .BAT files, the executing process is started, and then Launch will continue, leaving the loading process to run independently. For other persist keys (including .CAB files), Launch will wait for the loading process to complete before continuing. This is important, for example, to ensure that a .CAB file is installed before the .EXE files from the .CAB file are run.
- Note that the auto-launch process can also launch batch files (*.BAT), executable files (*.EXE), registry setting files (*.REG), or sound files (*.WAV). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Note: Registry entries may vary depending on software revision level and options ordered with the HX3.

LAUNCH.EXE and Persistent Storage

If any of the following directories are created in the System folder, Launch automatically copies all of the files in these directories to the respective folder on the flash drive:

- AppMgr
- Desktop
- Favorites
- Fonts
- Help
- Programs
- Recent

*Note: Files in the Startup folder are executed, but only from **System > Startup**. They are not copied to another folder.*

REGEDIT.EXE

Registry Editor – Use caution when editing the Registry and make a backup copy of the registry before changes are made.

REGLOAD.EXE

Double-tapping a registry settings file (e.g., REG) causes RegLoad to open the file and make the indicated settings in the registry. This is similar to how RegEdit works on a desktop PC. The .REG file format is the same as on the desktop PC.

REGDUMP.EXE

Registry dump – Saves a copy of the registry as a text file. The file, REG.TXT, is located in the root folder.

The REG.TXT file is not saved in persistent storage. To use the REG.TXT file as a reference in the event of a , copy the file to the System folder on the HX3 or store a copy of the REG.TXT file on a PC.

WARMBOOT.EXE

Double click this file to warm boot the computer (i.e., all RAM is preserved). It automatically saves the registry before rebooting which means configuration changes are not lost.

WAVPLAY.EXE

Double tapping a sound file (e.g., WAV) causes WavPlay to open the file and run it in the background.

Command-line Utilities

Command line utilities can be executed by **Start > Run >** [program name].

COLDBOOT.EXE

Command line utility which performs a cold boot (all RAM is erased).

Passwords are lost upon cold boot. If a password is set, that password must be entered to begin the cold boot power cycle process.

PrtScrn.EXE

Command line utility which performs a screen print and saves the file in .BMP format in the \System folder. Tap **Start > Run** and type **prtscrn** and tap **OK**, or press **Enter**. There is a 10 second delay before the screen print is made. The device beeps and the screen captured file (scrnnnnn.bmp) is placed in the \System folder. The numeric filename is incremented by 1 each time the PrtScrn function is activated. The command is not case-sensitive.

Warmboot Notes

- The wireless client connects automatically during each reboot.
- Bluetooth re-connects to nearby paired devices automatically at the conclusion of each reboot.
- If installed and pre-configured, Wavelink Avalanche connects remotely and downloads updates automatically during each reboot.

Desktop

For general use instruction, refer to commercially available Windows CE user's guides or the Windows on-line Help application installed in the mobile device.

The HX3 Desktop appearance is similar to that of a desktop PC running Windows XP.

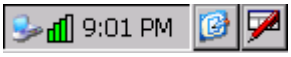
Note: HX3 applications, operating system settings and control panels can be viewed and edited / updated using LXEConnect and ActiveSync on a host computer cabled to the HX3.

Desktop Icons

At a minimum, the desktop displays icons for My Device, Internet Explorer and the Recycle Bin. Following are a few of the other icons that may be on the HX3 Desktop..

Icon	Function
	Access files and programs.
	Storage for files that are to be deleted.
	Discover and then pair with nearby discoverable Bluetooth devices.
	Storage for downloaded files / applications.
	Connect to the Internet/intranet.
	Used for accessing the appropriate wireless configuration, SCU (Summit Client Utility).
	A shortcut to the Remote Desktop Configuration utility.
	Wavelink® Avalanche Mobility Center™ (Avalanche MC) is a remote client management system that is designed to distribute software and configuration updates to monitored devices. The enabler for Wavelink Avalanche is loaded on the HX3 but not installed. When the enabler is installed this icon is displayed on the desktop.
	Tapping the desktop icon displays information on the Java version installed. Files can be accessed by tapping **Start > Programs > JEM-CE**. Doubletap the EVM icon to open the EVM Console. A folder of Java examples and Plug-ins is also installed with the Java option. Java applications running on the mobile device are not supported.
	Start button. Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help or run programs.

Taskbar



The number and type of icons displayed are based on the device type, installed options and configuration of the HX3.

Taskbar Icons

As HX3 devices and applications open and change state, icons are placed in the Taskbar. In most cases, tapping the icon in the Taskbar opens the related application.

Refer to **Start > Help** for an explanation of standard Windows CE taskbar icons.

Following are a few of the HX3 unique taskbar icons that may appear in the Taskbar. These icons are in addition to the Windows CE taskbar icons.

Icon	Function
	Battery charge indicator. Percent of battery charge is indicated.
	External power connected
	Click this icon to return to the Desktop.
	Input method, keyboard / input panel
	CapsLock active

My Device Folders

Folder	Description	Preserved upon Reboot?
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Network	Mounted network drive	No
Program Files	Applications	No
System	Internal SD Flash Card (CAB file storage)	Yes
Temp	Location for temporary files	No
Windows	Operating System in Secure Storage	No

Wavelink Avalanche Enabler (Option)

Note: If the user is NOT using Wavelink Avalanche to manage their mobile device, the Enabler should not be installed on the mobile device(s).

The following features are supported by the Wavelink Avalanche Enabler when used in conjunction with the Avalanche Manager.

After configuration, Enabler files are installed upon initial bootup and after a hard reset. Network parameter configuration is supported for:

- IP address: DHCP or static IP
- RF network SSID
- DNS hosts (primary, secondary, tertiary)
- Subnet mask
- Enabler update

Related Manual: *Using Wavelink Avalanche*

The HX3 has the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped The installation files are located in the System folder on CE devices. The installation application must be run manually the first time Avalanche is used.

After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the *Avalanche Update Settings* panel through the *Enabler Interface*.

Internet Explorer

Start > Programs > Internet Explorer

This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the "?" button to access Internet Explorer Help.

Start Menu Program Options

The following list represents the factory default program installation. Your system may contain different items from those shown below, based on the software and hardware options purchased.

Communication

Stores Network communication options.

ActiveSync

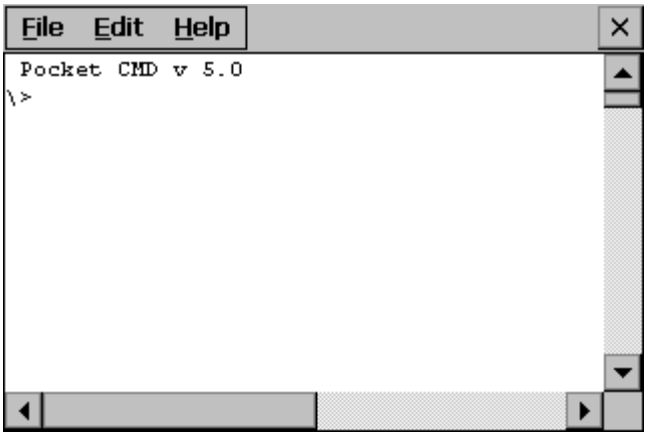
Transfer files between a HX3 and a host computer. ActiveSync is pre-loaded on the HX3. Using Microsoft ActiveSync you can copy files from your HX3 to your desktop computer , and vice versa. Once an ActiveSync relationship (partnership) has been established with Connect (on a host computer), ActiveSync will synchronize using the wireless link, serial port, or USB to the HX3.

Start FTP Server / Stop FTP Server

Begin and end connection to FTP server. These shortcuts call the Services Manager to start and stop the FTP server. The server defaults to Off (for security) unless it is explicitly turned on from the menu.

Command Prompt

The command line interface in a separate window.



Type help cmd at the command prompt to view valid Pocket PC (Console) commands. Exit the command prompt by typing exit at the command prompt or tap **File > Close**.

Internet Explorer

Access web pages on the Internet/Intranet. This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the ? button to access Internet Explorer Help.

Microsoft WordPad

Opens an ASCII notepad. Create and edit documents and templates in WordPad, using buttons and menu commands that are similar to those used in the desktop PC version of Microsoft WordPad. By default WordPad files are saved as .PWD files. Documents can be saved in other formats e.g., .RTF or .DOC. Tap the ? button to access WordPad Help.

Remote Desktop Connection

Log on to a Windows Terminal Server. There are few changes in the Windows CE version of Remote Desktop Connection as it relates to the general desktop Windows PC Microsoft Remote Desktop Connection options. If installed, Remote Desktop Connection on the HX3 can be accessed by **Start > Programs > Remote Desktop Connection**. Select a computer from the drop down list or enter a host name and tap the Connect button. Tap the Options >> button to access the General, Display, Local Resources, Programs and Experience tabs. Tap the ? button to access Remote Desktop Connection Help.

Settings

Access to all Control Panels, a shortcut to the Network and Dialup Control Panel and access to Taskbar options.

Summit

Set Summit radio / network parameters. Use this option to set up radio client profiles. The Summit Control Panel can also be accessed by double clicking the Summit icon in the taskbar or on the desktop. The Certs option displays a readme file containing details on how the Summit Configuration Utility (SCU) handles certificates for WPA authentication.

Wavelink Avalanche

Option. Remote management for networked devices.

Windows Explorer

File management program. There are a few changes in the Windows CE version of Windows Explorer as it relates to the general desktop PC Windows Explorer options. Tap the “?” button to access Windows Explorer Help.

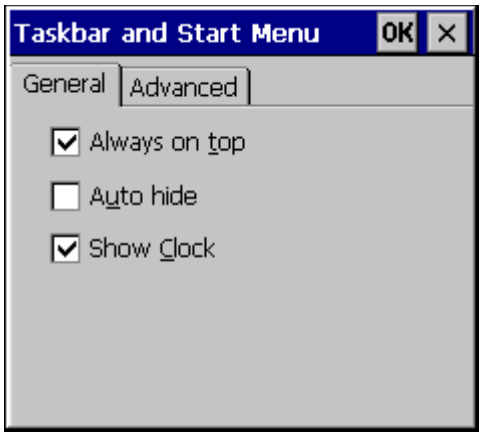
Taskbar

There are a few changes in the Windows CE version of Taskbar as it relates to the general desktop PC Windows Taskbar options. When the taskbar is auto hidden, press the Ctrl key then the Esc key to make the Start button appear. Clicking the Taskbar option on the Settings menu displays the Taskbar General tab and the Taskbar Advanced tab.

Note: HX3 applications, operating system settings and control panels can be viewed and edited / updated using LXEConnect and ActiveSync on a host computer cabled to the HX3.

General Tab

Setting	Default
Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled



Advanced Tab

Expand Control Panel

Tap the check box to have the Control Panel folders appear in drop down menu format from the **Settings > Control Panel** menu option.

Clear Contents of Document Folder

Tap the Clear button to remove the contents of the Document folder.

HX3 OS Upgrade

Depending on the size of the operating system, the total time required for a successful upgrade may require several minutes.

The OS upgrade files are unique to your HX3 physical configuration and date of manufacture. OS upgrade files designed for one device configuration should not be used on a different device configuration.

Preparation

1. Contact Customer Support (page 14-1) to get the OS upgrade files.
2. Put the upgrade files on a host computer with ActiveSync and USB capability.
3. Use ActiveSync to back up HX3 user files and store them elsewhere before beginning an upgrade on the HX3.
4. Maintain an uninterrupted AC/DC power source to the HX3 throughout this process.

The SD / CF card with the OS and system files must be present for the HX3 to boot. Removal or installation of SD or CF cards must be performed on a clean, well-lit surface.

Always perform OS updates when the HX3 has a dependable external power source connected to the HX3 and/or a fully charged tethered battery.

Procedure

1. Verify a dependable power source is applied to the HX3 and will stay connected during the upgrade procedure.
2. Establish an ActiveSync connection between the HX3 and a host computer.
3. Download the OS files from the desktop/laptop to the HX3 System folder.
4. During the file copy process to the HX3 System folder, when asked “Overwrite?”, select Yes to All.
5. Review the files that were downloaded to the System folder.
6. Restart the HX3.
7. Disconnect from ActiveSync.
8. When the OS finishes loading, check the OS update version by selecting **Start > Settings > Control Panel > About > Software** tab.
9. Upgrade Help

Contact Customer Support (page 14-1) for re-imaging options if the HX3 won't boot up after the upgrade is finished.

Warning: Opening the device e.g., removing endcaps or access panels, etc. could void the user's authority to operate this equipment.

Battery State and OS Upgrade

A fully charged main battery must be cabled to the HX3 prior to reflashing or upgrading the operating system. A prompt may appear when the battery reaches Critical Low that informs the user there is not enough power in the main battery to perform the upgrade.

The operating system will not be able to execute the OS update when the battery level is too low (25% or less), as there is a high risk that the power remaining in the battery expires when executing the upgrade and the HX3 will be left in an inoperable state.

When main battery power level is too low, connect external power to the HX3 before performing the upgrade procedure. Do not disconnect external power before the upgrade process is complete.

Control Panel

Note: Although the HX3 has no display or alphanumeric keypad, HX3 control panels can be viewed and settings manipulated using LXEConnect and ActiveSync on a connected host computer.

Tap the ? button for Help when changing HX3 Control Panel options.

Option	Function
About (page 5-19)	Software, hardware, versions and network IP. No user intervention allowed.
Battery (page 5-20)	View voltage and status of the main and backup (or internal) batteries.
Bluetooth	Set the parameters for Bluetooth device connections. See Bluetooth Configuration (page 6-1).
Certificates (page 5-21)	Manage digital certificates used for secure communication.
Date / Time (page 5-22)	Set Date, Time, Time Zone, and Daylight Savings.
Device Management (page 5-22)	Connection setup for Microsoft Systems Management Server.
Dialing (page 5-23)	Connection setup for modem attached to COM port or Compact Flash slot.
Display (page 5-24)	Set background graphic and scheme. Set touch screen and keypad backlight properties and timers.
HX2-3 Options (page 5-26)	Set various device specific configuration options.
Installed Programs (page 5-28)	View the list of installed programs. In some OS versions this panel replaced Remove Programs.
Keyboard (page 5-29)	Select a Key Map (or font). Set key repeat delay and key repeat rate.
KeyPad (page 5-30)	Configure Alpha key, KeyMap keys, RunCmd and LaunchApp.
License Viewer (page 5-35)	Displays license information for installed licensed applications.
Mixer (page 5-36)	Adjust the input and output parameters – volume, sidetone, and record gain, for headphone, software and microphone.
Mouse (page 5-38)	Set the double-tap sensitivity for stylus taps on the touch screen.
Network and Dialup Options (page 5-39)	Set network driver properties and network access properties.
Network Capture (page 5-40)	Set network logging options.
Owner (page 5-43)	Set the mobile device owner details (name, phone, etc.). Enter notes. Enable / disable Owner display parameters. Enter Network ID for the device – user name, password, domain.
Password (page 5-44)	Set OS access password properties for signon and/or screen saver.
PC Connection (page 5-45)	Control the connection between the mobile device and a local desktop or laptop computer.
Power (page 5-46)	Set Power scheme properties. Review device status and properties.
Regional and Language Settings (page 5-48)	Set appearance of numbers, currency, time and date based on country region and language settings.
Remove Programs (page 5-49)	This panel has been replaced by Installed Programs
Scanner	Scan Wedge utility. Set scanner key wedge, scanner port, and imager LED illumination options. Assign baud rate, parity, stop bits and data bits for COM1 port. Assign scanned bar code data manipulation parameters. See Bar Code Scanner Wedge (page 7-1).
System (page 5-50)	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description. Review copyright notices.
Volume and Sounds (page 5-52)	Enable / disable volume and sounds. Set volume parameters and assign sound WAV files to events.
Wi-Fi (page 5-52)	Set the parameters for a Summit client. See Wireless Network Configuration (page 9-1).

About

Start > Settings > Control Panel > About

The data cannot be edited by the HX3 user on these panels.

Tab	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, FPGA Version and Language. Language indicates localized version.
Hardware	CPU Type, Codec Type, FPGA Version, Scanner type, Display, Flash memory, and DRAM memory
Versions	Revision level of software modules and .NET Compact Framework Version.
Network IP	Current network connection IP and MAC address. Only the first 2 network ports are shown (usually radio and ActiveSync).

Version window information is retrieved from the registry.

Version Tab and the Registry

Modify the Registry using the Registry Editor. Use caution when editing the Registry and make a backup copy of the registry before changes are made.

The registry settings for the Version tab are under HKEY_LOCAL_MACHINE \ Software \ LXE \ Version in the registry.

To add a user application to the Version panel, create a new string value under the HKLM\Software\LXE\Version key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window.

Version strings can be equal to or less than 254 characters. Because the strings are displayed in a text box, any number can be accommodated, up to the 64K byte text box limitation.

Languages

The Software tab displays any languages built into the OS image. The languages built into the OS image are noted in the Language section of this tab:

- English only – No additional languages are built into the OS
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean

The above listed Asian languages are ordered separately and built-in to the OS image. Built-in languages are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian languages are available in the (English only) default (extended) fonts.

Identifying Software Versions

The Versions tab displays the versions of many of the software programs installed. Not all installed software is included in this list and the list varies depending on the applications loaded on the HX3. The Image line displays the revision of the system software installed. Refer to the last three digits to determine the revision level.

MAC Address

The Network IP tab displays the MAC address of the network card.

Battery

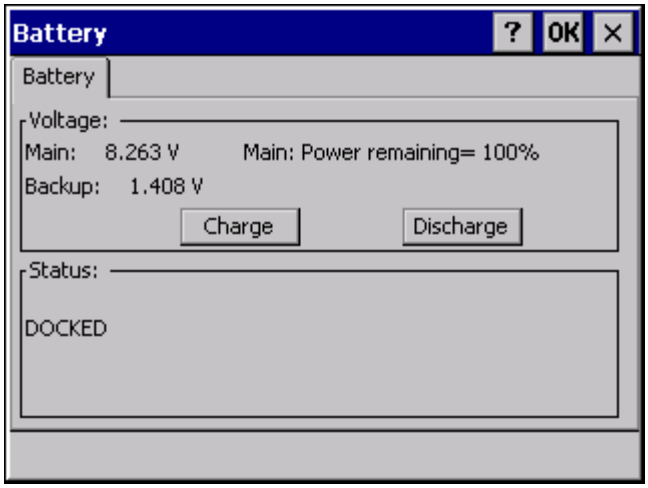
Start > Settings > Control Panel > Battery

This panel is used to view the status and percentage of power remaining in the HX3 Main battery.

	The battery gas gauge icon resides in the system tray and shows four levels of charge – 100%, 75%, 50%, 25%. At a point below 25%, the system status LED will turn red and the gas gauge icon will turn red indicating the battery is low.

Jacked is shown in the Status box when the Main battery is receiving external power.

The main battery is charged/recharged when the HX3 is docked in a powered cradle or directly cabled to an external power source.



The backup battery draws power from the Main battery to maintain a charge. The backup battery voltage and percentage of power fluctuate continuously.

When there is no Main battery in the unit, the backup battery begins to discharge as it maintains RAM and other vital settings. After a Main battery is installed, the backup battery begins to draw power from the Main battery again.

Note: Frequent connection to an external power source, if feasible, is recommended to maintain backup battery charge status as the backup battery cannot be recharged by a dead or missing main battery.

Backup Battery Maintenance

Discharge and recharge the backup battery twice a year. Use the Charge or Discharge buttons to charge and discharge the backup battery:

To Charge

Tap the Charge button. The Discharge button text changes to "Off". When the backup battery is charging, tap the Off button to stop the Charge process.

To Discharge

Tap the Discharge button. The Charge button text changes to "Off". When the backup battery is discharging, tap the Off button to stop the Discharge process.

Certificates

Start > Settings > Control Panel > Certificates

Manage digital certificates used for secure communication. Digital certificates are date sensitive. If the date on the HX3 is incorrect, wireless authentication will fail.

The Certificates stores lists the certificates trusted by the HX3 mobile device user.

These values may change based on the type of network security resident in the client, access point or the host system.

Tap the Import button to import a digital certificate file.

Tap the View button to view a highlighted digital certificate.

Tap the Remove button to remove highlighted certificate files.

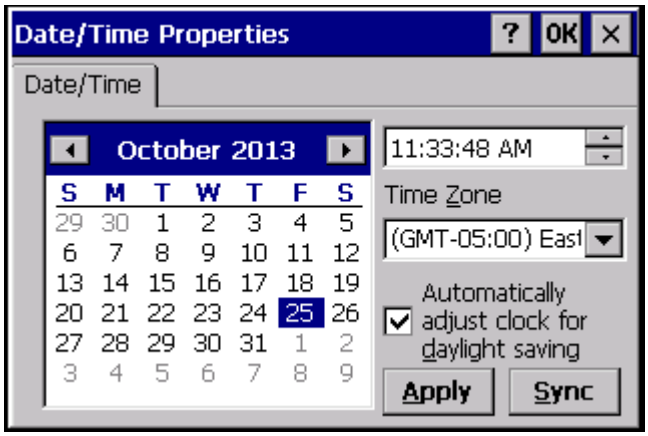
Tap the ? button and follow the instructions in the Windows CE Help file when working with trusted authorities and digital certificates.

Date / Time

Start > Settings > Control Panel > Date/Time - or - Time in Desktop Taskbar

Use this HX3 panel to set Date, Time, Time Zone, and assign a Daylight Savings location.

Setting	Default
Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Enabled



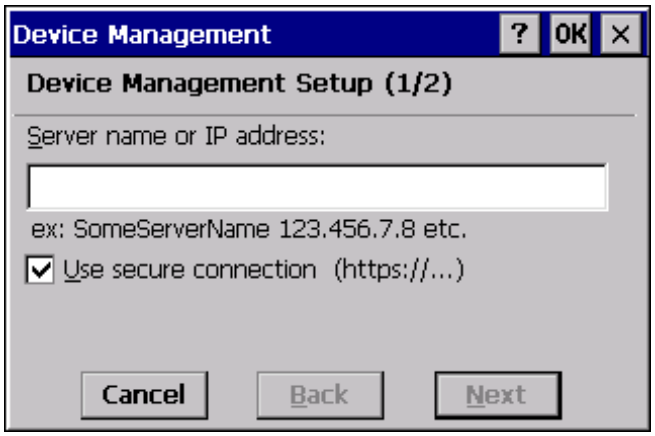
There is very little functional change from general desktop or laptop Date/Time Properties options.

Double-tapping the time displayed in the Desktop Taskbar causes the Date/Time Properties screen to appear. The Sync button (if available) activates a utility that will set the clock using a network time server.

Device Management

Start > Settings > Control Panel > Device Management

Allows a Device Management client (the device equipped with a Microsoft Windows CE operating system) to work with a Microsoft Systems Management Server.



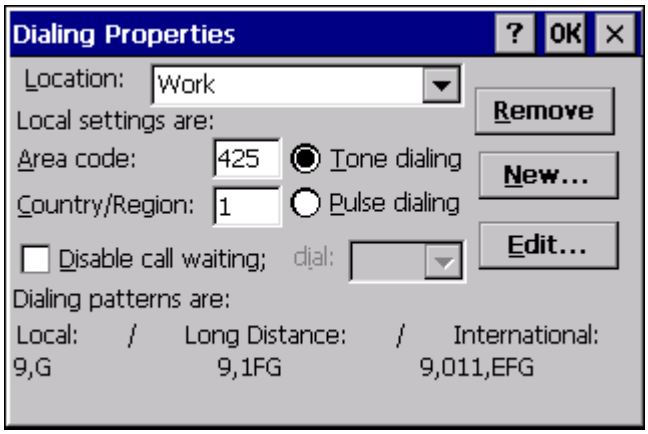
Specify the server name or IP address of management server and check the check box if a secure connection is to be used. Refer to the Microsoft.com website for more information on device management for Windows CE equipped devices.

Dialing

Start > Settings > Control Panel > Dialing

Set dialup properties for internal modems (not supplied or supported on the HX3).

Setting	Default
Location	Work
Area Code	425
Tone Dialing	Enabled
Country/Region	1
Disable Call Waiting	Disabled (blank)



Display

Start > Settings > Control Panel > Display

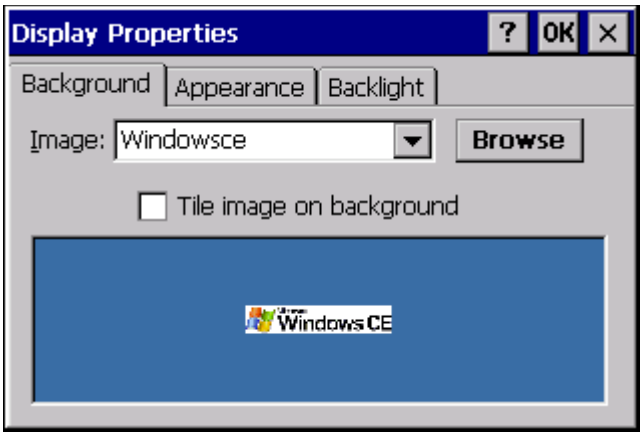
The display might also called the touch screen.

Select the desktop background image and appearance scheme for the HX3. Using the options on the Backlight tab, set the display backlight and keypad backlight timers when running on battery or external power.

Adjust the settings and tap the OK button to save the changes. Saved changes take effect immediately.

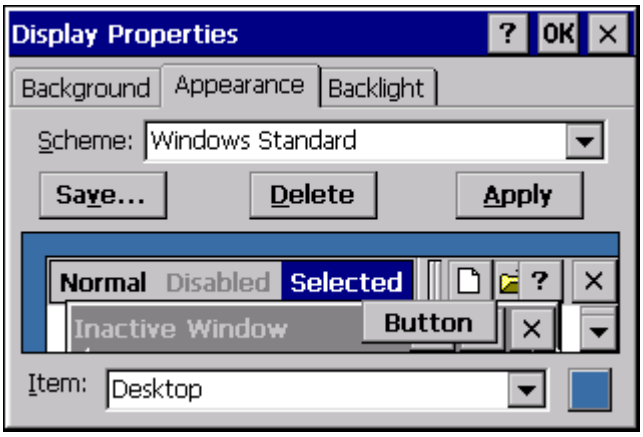
Setting	Default
Background tab	
Image	Windows CE
Image on background	Disabled
Appearance tab	
Schemes	Windows Standard
Backlight tab	
Battery power	Never
External power and user idle	Never

Background



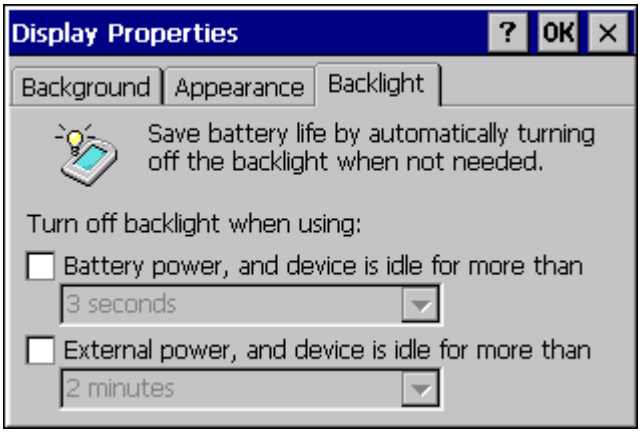
There is very little change from general desktop PC Display Properties / Background options. Select an image from the dropdown list (or tap the Browse button to select an image from another folder) to display on the Desktop, and then tap the OK button to save the change. The change takes effect immediately.

Appearance



There is very little change from general desktop PC Appearance options. Select a scheme from the dropdown list and make changes to the parameters. The default is High Contrast White for monochrome displays and Windows Standard for color displays. Tap the Save button to save any changes, renaming the scheme if desired. Tap the Delete button to delete schemes. Tap the Apply button to apply the selected scheme to the display.

Backlight



The backlight settings use the default timeouts and is synchronized to the User Idle setting in the Schemes tab in the Power control panel.

When the backlight timer expires, the touch screen backlight is dimmed, not turned off. When both checkboxes are unchecked, the backlight never turns off (or dims).

Default values are disabled for battery and external power. By default the backlight is always on.

HX2-3 Options

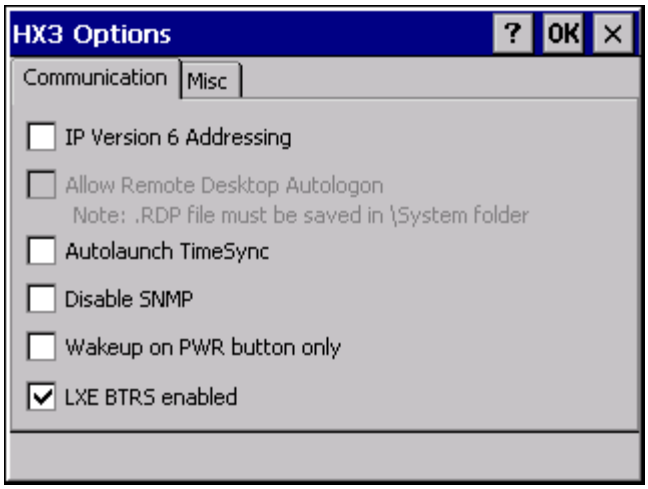
Start > Settings > Control Panel > HX2-3 Options

Set options such as IP V6 and time sync.

It may be necessary to warmboot the HX3 after making desired changes. A pop up window indicates if a warmboot is required.

Communication

Options on this tab configure communication options for the HX3.



Enable TCP/IP Version 6

By default, IPv6 is disabled on the HX3. Click this check box to enable IPv6.

Autolaunch TimeSync

By default, TimeSync does not automatically run on the HX3. To enable TimeSync to run automatically on the HX3, click this check box.

Synchronize with a Local Time Server

By default, GrabTime synchronizes via an Internet connection. To synchronize with a local time server:

1. Use ActiveSync to copy GrabTime.ini from the **My Device > Windows** folder on the mobile device to the host PC.
2. Edit the copy of GrabTime.ini on the host PC. Add the local time server's domain name to the beginning of the list of servers. You can optionally delete the remainder of the list.
3. Copy the modified GrabTime.ini file to the **My Device > System** folder on the mobile device.

The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. System/Grabtime.ini also persists after a coldboot; Windows/Grabtime.ini does not persist.

Disable SNMP

By default, the SNMP agent is running on the HX3. To disable the SNMP agent, check this box.

Wakeup on PWR Button Only

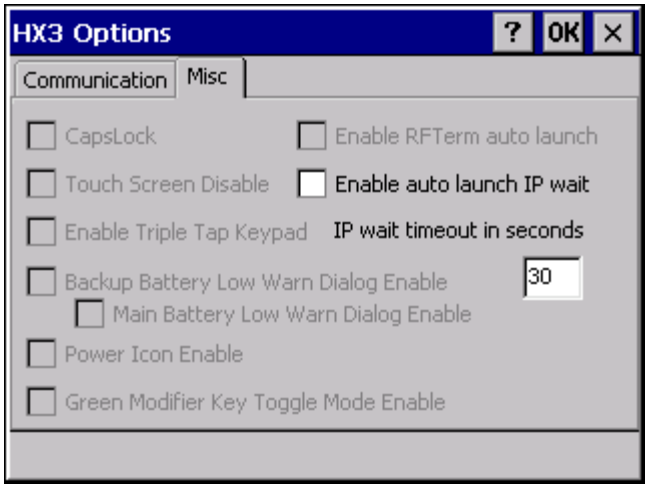
When this option is checked, the only wake up event is a press of the power button. When unchecked (default) normal wake up events for the HX3 are enabled.

LXE BTRS Enabled

By default, the HX3 uses proprietary handshaking designed for the Honeywell Bluetooth Ring Scanner. Uncheck this box to use the HX3 with a third party Bluetooth scanner.

Misc

Options on this tab configure device specific options. Note that options not available on the HX3 are dimmed or grayed out.



Enable Auto Launch IP Wait

When enabled, this feature works as follows:

1. After the radio .CAB file is unpacked, the Launch program waits for the radio driver to load and for the radio to connect and obtain an IP address.
2. During the wait, a message window is displayed containing the NDIS communication messages up to and including the display of the valid IP address.
3. After the IP address is obtained, the message window is displayed for one second and then removed.
4. Launch completes its normal task path, unpacking any remaining .CAB files and completing any remaining tasks.
5. If an IP address is not obtained within the specified timeout period (see below), Launch completes its normal task path.

The default is unchecked (disabled). Launch does not wait for an IP address.

IP Wait Timeout

This parameter specifies the maximum time period Launch waits for a valid IP address before completing any remaining tasks. The timeout can be from 1 to 60 seconds. The default is 30 seconds.

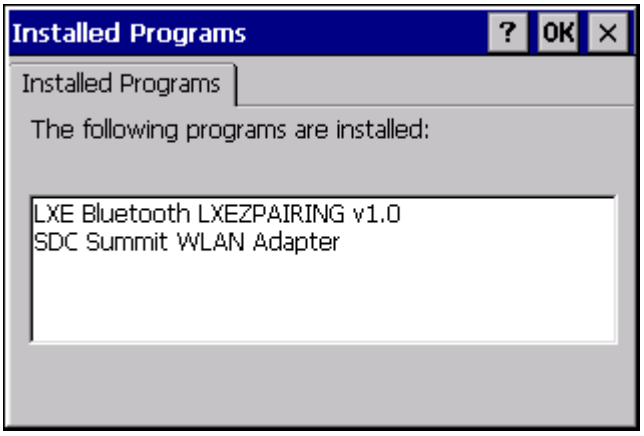
Installed Programs

Start > Settings > Control Panel > Installed Programs

Note: This panel shows the programs installed in RAM.

View the list of installed programs. No user interaction is required or allowed.

In some OS versions, this panel replaces Remove Programs.



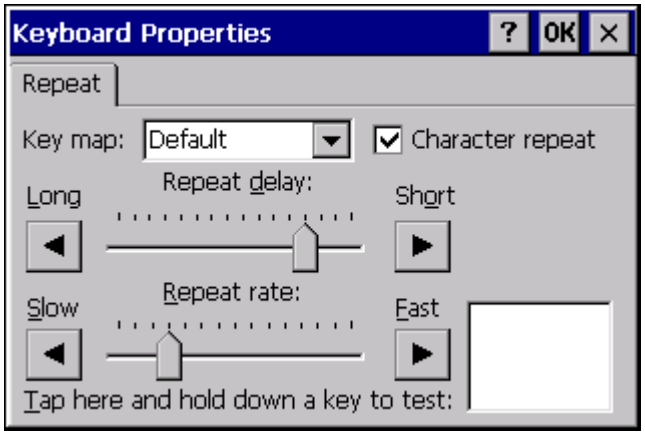
Note: Contact Customer Support (page 14-1) if installed programs must be deleted.

Keyboard

Start > Settings > Control Panel > Keyboard

Set keypad key map, keypad key repeat delay, and key repeat rate.

Setting	Default
Key map	Default (or Default HX3)
Repeat character	Enable
Repeat Delay	Short
Repeat Rate	Slow



Select a key map using the drop-down list. Adjust the character repeat settings and tap the OK button to save the changes.

When new key maps, or fonts, are added to the registry, they are available immediately and the font name is in the Keyboard Properties Key map dropdown list. Only one font at a time can be selected. The fonts affect the screen display, they do not affect any virtual (touch screen) key taps.

Languages

Loads are available in the following languages (in separate part numbers) for each language: Simplified Chinese, Traditional Chinese, Korean, Japanese. Tahoma font is on every unit and includes English (default), European (French, Spanish, German, Portuguese), Scandinavian languages, Arabic, Cyrillic, Greek, Hebrew, and Thai.

KeyPad

Start > Settings > Control Panel > KeyPad Icon

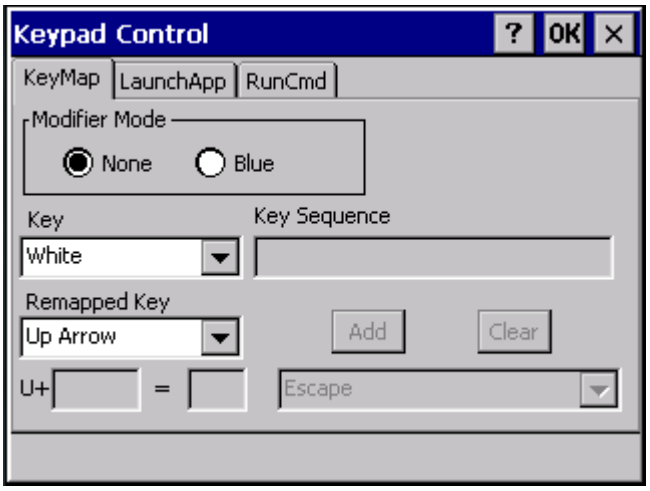
Use this control panel option to assign key functions to mappable keys available on your HX3, determine application launch sequences and program command Run sequences.

Setting	Default	
KeyMap		
Modifier Mode	None	
Key	White	Remap to – Up Arrow
Edit String	Field Exit	String – Empty
Unicode	Any Unicode value	String of 4 hex characters - Empty
LaunchApp		
App1	Empty	
App2	Empty	
App3	Empty	
App4	Empty	
App/Opt	EXE	
RunCmd		
Cmd1	Empty	
Cmd2	Empty	
Cmd3	Empty	
Cmd4	Empty	
File/Parm	FILE	

The KeyPad panels can be used to perform the following functions:

- Remap a Key to a Single Key (page 5-31).
- Remap a Key to a Key to a Unicode Value (page 5-31).
- Remap a Key to a Key Sequence (page 5-31)
- Remap a Key to a Key to a Sequence of Unicode Values (page 5-32).
- Remap a Key to Launch an Application (page 5-32).
- Remap a Key to Run a Command (page 5-32).

Note: KeyPad Control Panel options LaunchApp and RunCmd do not inter-relate with similarly-named options contained in other Control Panel applets.



Assign settings by clicking radio buttons and selecting keys from the drop down boxes. Tap the OK button when finished. The changes take effect immediately.

Remap a Key to a Single Key

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select the value from the remapped key from the Remapped Key pulldown list.
4. Click OK to save the result and close the control panel.

Remap a Key to a Key to a Unicode Value

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Unicode from the Remapped Key pulldown list.
4. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the left text box and the Unicode character is displayed in the right text box.
5. Click OK to save the result and close the control panel.

Remap a Key to a Key Sequence

Up to 16 keys may be specified for the key sequence. The sequence can consist of keys and Unicode values.

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Key Sequence from the Remapped Key pulldown list.
4. Select the first key for the multiple key sequence from the pulldown list.
5. Press the Add button to add the key to the multiple key sequence shown in the Key Sequence box.
6. Repeat steps 4 and 5 until all keys desired have been added to the key sequence. If necessary, use the Clear button to erase all entries in the Key Sequence box.
7. Click OK to save the result and close the control panel.

Note: A key can only be used once in a multiple key sequence. For example, an F1 key added to a key sequence means an F1 key cannot be used again in the same key sequence.

Remap a Key to a Key to a Sequence of Unicode Values

Up to 16 Unicode values may be specified for the key sequence. The sequence can consist of keys and Unicode values.

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Key Sequence from the Remapped Key pulldown list.
4. Select Unicode from the Key Sequence pulldown list.
5. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the left text box and the Unicode character is displayed in the right text box.
6. Press the Add button to add the key to the multiple key sequence shown in the Key Sequence box.
7. Repeat steps 4 through 6 until all desired characters have been added to the key sequence. If necessary, use the Clear button to erase all entries in the Key Sequence box.
8. Click OK to save the result and close the control panel.

Remap a Key to Launch an Application

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Launch App1-4 from the remapped key from the Remapped Key pulldown list.
4. Click on tthe LaunchApp tab.
5. Make sure the EXE radio button is selected.
6. In the text box (App1-4) corresponding to the number selected for Launch App1-4, enter the application to launch.
7. If any parameters are needed for the application, click on the OPT radio button. This clears the text box (though the application name is saved). Enter the desired parameters in the appropriate text box.
8. Click OK to save the result and close the control panel.
9. If the KeyMap tab is accessed again, the application plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

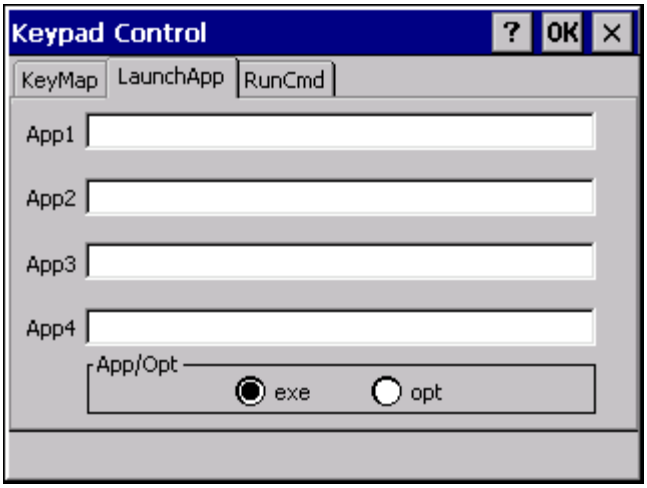
Remap a Key to Run a Command

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select RunCmd 1-4 from the remapped key from the Remapped Key pulldown list.
4. Click on the RunCmd tab.
5. Make sure the FILE radio button is selected.
6. In the text box (Cmd1-4) corresponding to the number selected for RunCmd1-4, enter the desired command.
7. If any parameters are needed for the command, click on the PARM radio button. This clears the text box (though the command is saved). Enter the desired parameters in the appropriate text box.
8. Click OK to save the result and close the control panel.
9. If the KeyMap tab is accessed again, the command plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

LaunchApp Tab

The default for all text boxes is Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the HX3 emits a single beep, if the launch is successful, it is silent.



The Launch App command is defined for use by system administrators. These instructions are parsed and executed directly by the keyboard driver.

1. Place the cursor in the text box next to the App you wish to run, e.g., App1, App2.
2. Enable the EXE radio button if the application is an EXE file.
3. Enter the name of the executable file.
4. Enable the OPT radio button to add options or parameters for the executable file in the same text box. Switching from EXE to OPT clears the text box (but the information previously entered is stored), allowing parameter entry.

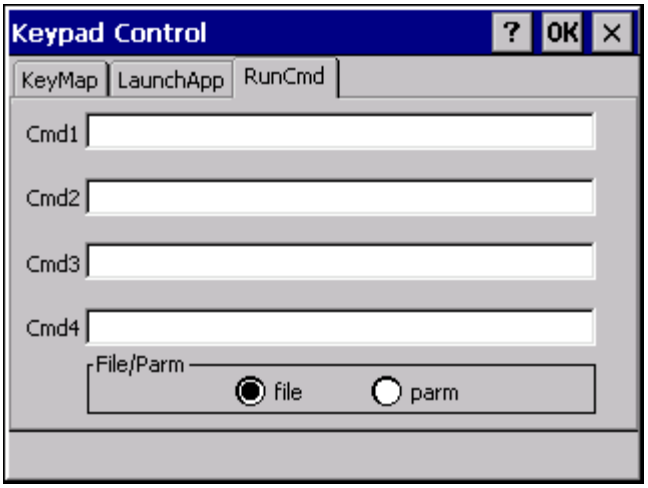
Tap the OK button when finished. The changes take effect immediately.

The result of the application (exe) and options (opt) entries are displayed on the KeyMap tab in the Key Sequence box when the key mapped to the LauchApp is selected.

RunCmd Tab

The default for all text boxes is Empty, Null or “ ”. The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the HX3 emits a single beep, if the launch is successful, the mobile device is silent.



The Run Cmd command is defined for use by system administrators. These instructions call the ShellExecuteEx API, which opens documents directly.

1. Place the cursor in the text box next to the Cmd you wish to run, e.g., Cmd1, Cmd2.
2. Enable the file radio button and enter the name of the file.
3. Enable the PARM radio button to add parameters for file/exe execution in the same text box.
4. Tap the OK button when finished. The changes take effect immediately.

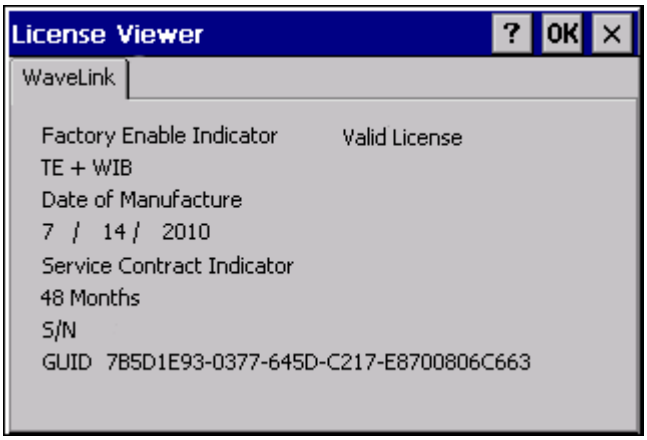
License Viewer

Start > Settings > Control Panel > License Viewer

Use this option to view software license registration details, and service contract length for an HX3. Information on the License Viewer tabs is unique for each HX3.

Note: Following image is a sample screen.

Note: Your License Viewer control panel may show more tabs, e.g., RFTerm, depending on the number of software applications running on the HX3 that require a license. Contact Customer Support (page 14-1) for software updates and releases as they become available.



Software and driver version information is located in the About control panel. Copyright information is located in the System control panel.

Mixer

Start > Settings > Control Panel > Mixer

The HX3 has a speaker and a microphone. They are active when a headset is not connected to the device.

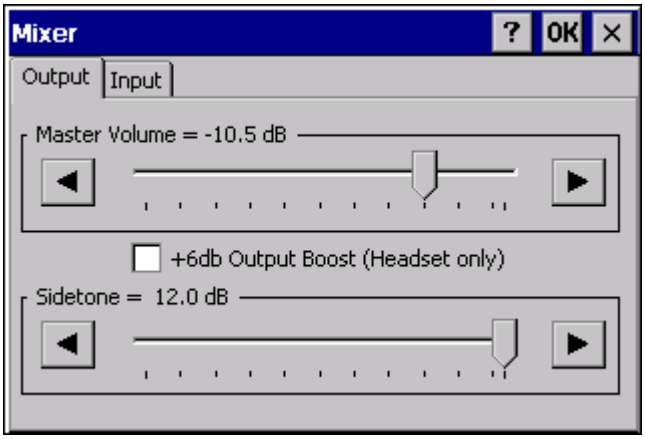
The microphone is located to the right of the oval logo at the top of the unit.

Use the settings on these panels to adjust the volume, record gain and sidetone for microphone input, speaker and speaker output.

Headsets can be enabled, disabled and selected using these panels.

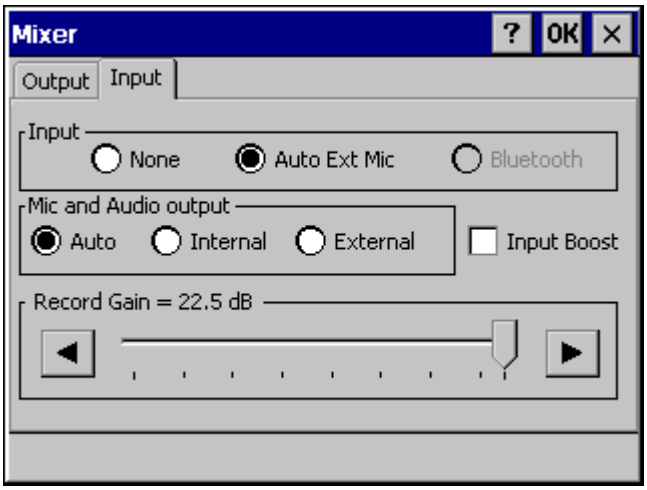
Setting	Default
Output tab	
Master Volume	-10.5 dB
+6db Output Boost (Headset only)	Disabled
Sidetone	12.0 dB
Input tab	
Input	Auto Ext Mic
Mic and Audio output	Auto
Input Boost	Disabled
Record Gain	22.5 dB

Output panel



Tap and hold the Output sliders and move them either left or right, or click the left and right arrows, to adjust Speaker volume decibel level.

Input Panel



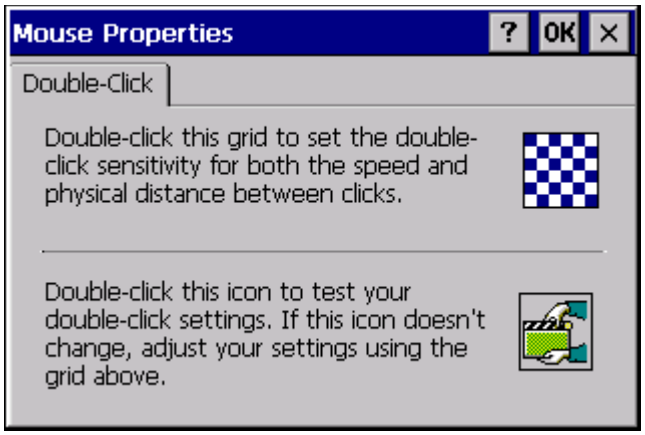
Option	Function
Input	Determines the audio input used (options available depend on the state of the Mic and Audio Output parameter): • None - No microphone is enabled. • Auto Ext Mic - (default) Automatically switch between internal microphone (when no cable is attached) and external microphone (when cable is attached) depending on presence of audio cable. • Internal Mic - Only use internal microphone. • External - Only use external microphone. • Bluetooth - Not available.
Mic and Audio Output	Determines the microphone and audio output source used: • Auto - (default) Automatically switch between internal microphone/speaker (when no cable is attached) and external microphone/headset (when cable is attached) depending on presence of audio cable • Internal - Internal speaker and microphone are enabled regardless of presence of audio cable. • External - External speaker and microphone are enabled regardless of presence of audio cable.
Input Boost	When checked (enabled) increases the sensitivity of the microphone (internal or headset) by 20 dB.
Record Gain	Tap and hold the slider and move it left and right to adjust. Or click the left and right arrow keys to adjust the slider. The default is 22.5 dB.

Mouse

Start > Settings > Control Panel > Mouse

Note: The HX3 does not have a touch screen. If the host computer has a touch screen, instructions using "tap" and "stylus" instead of "click" and "mouse" apply.

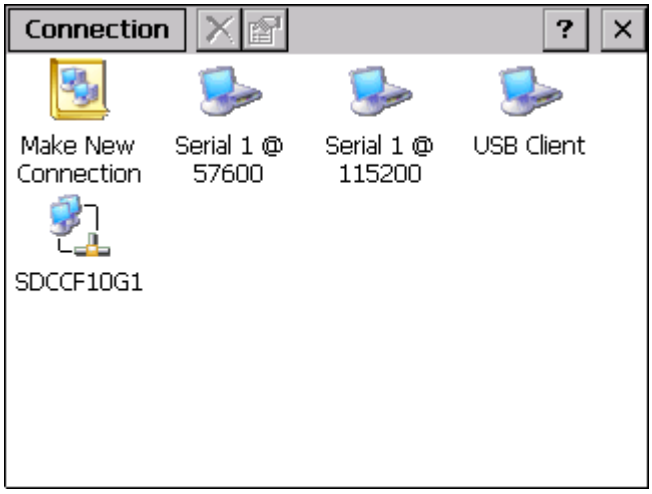
Note: Use this option to set the double-tap sensitivity for stylus taps on the HX3 touch screen.



Network and Dialup Options

Start > Settings > Control Panel > Network and Dialup Connections

Set HX3 network driver properties and network access properties. Select a connection to use, or create a new connection.



Create a New Connection

1. On the mobile device, select **Start > Settings > Control Panel > Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the connection you want does not exist, double-tap **Make New Connection**.
3. Give the new connection an appropriate name (My Connection @ 9600, etc.). Tap the Direct Connection radio button. Tap the Next button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Tap the **Configure...** button.
6. Under the Port Settings tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the Call Options tab, be sure to turn off Wait for dial tone, since a direct connection will not have a dial tone. Set the timeout parameter (default is 5 seconds). Tap OK.
8. TCP/IP Settings should not need to change from defaults. Tap the Finish button to create the new connection.
9. Close the Remote Networking window.
10. To activate the new connection select **Start > Settings > Control Panel > PC Connection** and tap the **Change Connection…** button.
11. The HX# only supports USB PC connections. Do not select any other type.
12. Select the new connection. Tap **OK** twice.
13. Close the Control Panel window.
14. Connect the desktop PC to the mobile device with the appropriate cable.
15. Click the desktop Connect icon to test the new connection.

You can activate the connection by double-tapping on the specific connection icon in the Remote Networking window, but this will only start an RAS (Remote Access Services) session, and does not start ActiveSync properly.

Network Capture

Start > Settings > Control Panel > Network Capture

Verify the date and time are correct before using the logging utilities to ensure meaningful data.

The Network Capture panels provide configuration options for logging utilities. Two types of logging are configurable:

Netlog is a Windows CE utility that monitors network traffic. Netlog creates a .CAP file that can be read using Microsoft Windows Network Monitor or any compatible tool that supports .CAP files.

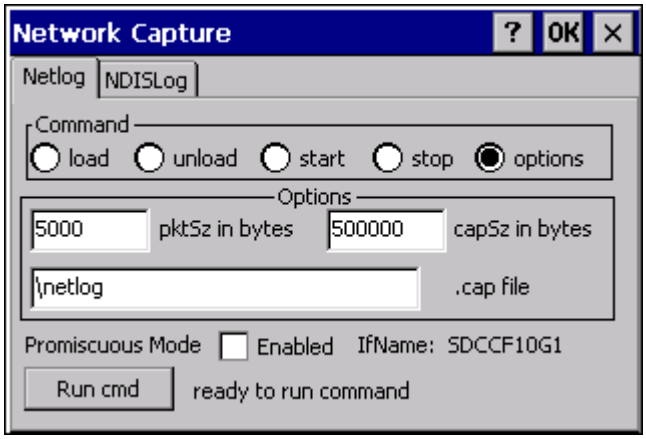
NDISLog monitors the NDIS interface between the Summit radio and the NDIS driver. This utility creates a .TXT log file.

Setting	Default
Netlog tab	
Command	options
pkt_size in bytes	5000
cap_size in bytes	500000
.cap file	\netlog
Promiscuous Mode	Disabled
NDISLog tab	
Command	stop
file	\ndislog.txt

Netlog

Use this control panel to configure the Netlog utility. By configuring Netlog using the control panel, Netlog remains running across a warmboot. However, note that:

- Netlog first stores data to a file named netlog0.cap, then netlog1.cap. Any time the current file reaches maximum size, Netlog switches to the other file.
- If the log file is stored in the root directory, any previous data is lost and a new log file started after the warm.boot
- If the log file is stored in \System, all previous data is saved across the warmboot.
- If Netlog is enabled across the warmboot, a series of brief popups may be displayed during the boot cycle. No user interaction is required.



Command

Command	Function
options	Specifies the option to perform. See the table below for the option parameters and values.
load	Loads and starts Netlog.
start	Starts the Netlog process of logging the network traffic.
stop	Stops Netlog from logging network traffic.
unload	Unloads Netlog.

Options

Options	Function
pkt_size in bytes	Specifies the maximum packet size captured in bytes. This option should only be run after you have called load and stop. Default is 5000.
cap_size in bytes	Specifies the maximum size of Netlog0.cap or Netlog1.cap in bytes. This option should only be run after you have called **load** and **stop**. Default is 500,000.
.cap file	Specifies the name of the file to which network traffic information is saved. This option should only be run after you have called **load** and **stop**. Default is \netlog.

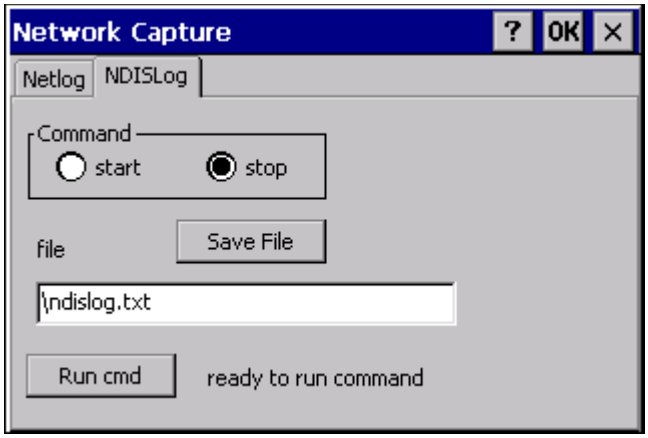
Run cmd

Performs the command selected. For example, to run Netlog and modify the packet size do the following:

1. Select load from the Commands list and click the Run cmd button.
2. Select stop from the Commands list and click the Run cmd button.
3. Select options from the Commands list, enter the new packet size in the Options list and click the Run cmd button.

NDISLog

NDISLog creates a .TXT file that can be viewed with any text editor program that supports .TXT files.



Command

Command	Function
start	Starts logging the network traffic.
stop	Stops logging network traffic.

file

Specifies the name of the file to which NDISLog information is stored.

Save File

Stores the file name.

Run cmd

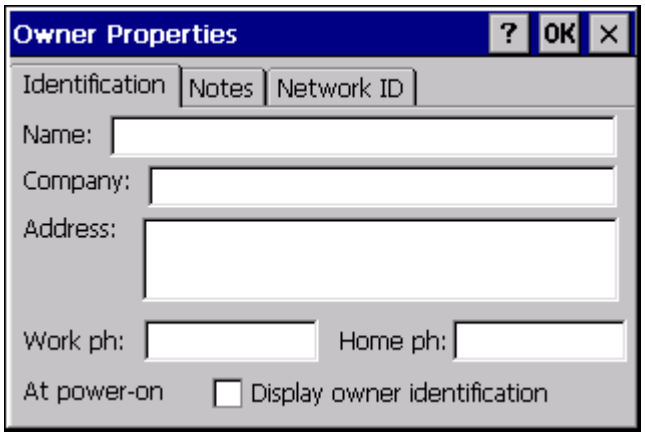
Performs the selected start or stop command.

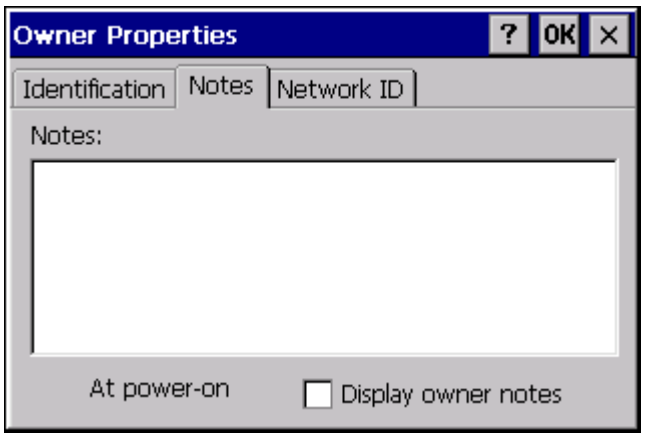
Owner

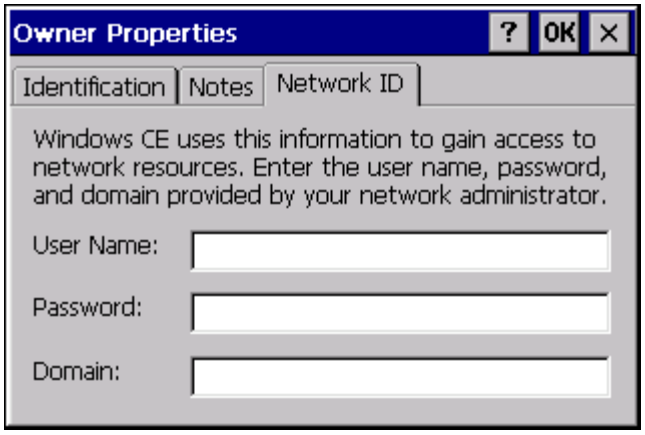
Start > Settings > Control Panel > Owner

Set the HX3 owner details. The Network ID is used when logging into a remote network.

Setting	Default
Identification tab	
Name	Blank
Company	Blank
Address	Blank
Telephones	Blank
Display owner ID at power-on	Disabled
Notes tab	
Notes	Blank
Display notes at power-on	Disabled
Network ID tab	
User Name	Blank
Password	Blank
Domain	Blank







Password

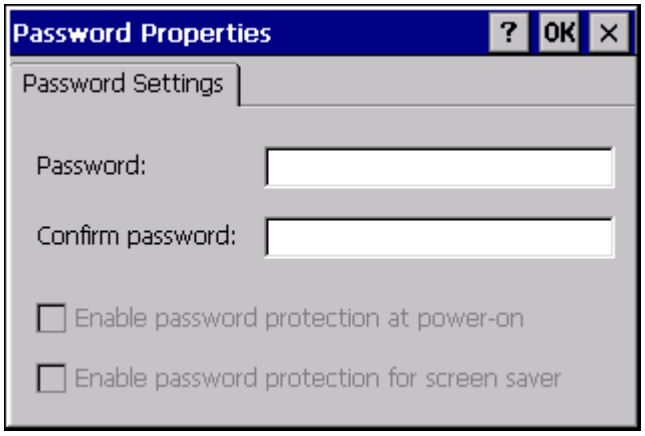
Start > Settings > Control Panel > Password

Use this panel to set HX3 user access to control panels and power up password properties.

Important: This password must be entered before performing a cold boot or cold reset.

If entering a power-on or screen saver password does not allow you to disable this password protection or perform a cold boot, contact Customer Support.

Setting	Default
Password	Blank
Enter password at Power On	Disabled
Enter password at Remote Desktop Screen Saver	Disabled



The password and password settings are saved during a warm boot and a cold boot. The screen saver password affects the Remote Desktop screen saver only. After a password is assigned and saved, each time a **Settings > Control Panel** option is selected, the user will be required to enter the password before the Control Panel will open. The screen saver password is the same as the power-on password. They are not set independently. A screen saver password cannot be created without first enabling the “Enable password protection at power-on” check box. The screen saver password is not automatically enabled when the “power-on” check box is enabled.

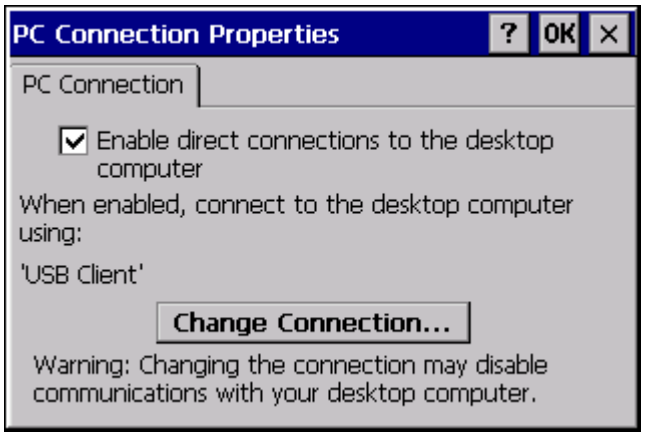
1. Enter the password in the Password text box, then press Tab and type the password again to confirm it.
2. Enable the power-on check box and, if desired, the screen saver check box.
3. A changed/saved password is in effect immediately.

PC Connection

Start > Settings > Control Panel > PC Connection

Use these options to control a cabled connection (USB, serial) between the HX3 and a nearby desktop/laptop computer.

Setting	Default
Enable direct connection	Enabled
Connect using	USB Client



- Unchecking the Enable direct connections check box disables ActiveSync on the HX3.
- Tap the Change Connection button to change the direct connect setting.
- Tap the drop-down box to view a list of pre-configured connection settings.

Note: The HX3 only supports the USB connection. Do not change the connection type or the ability to connect with the HX3 may be lost.

Power

Start > Settings > Control Panel > Power

The HX3 power mode timers are cumulative. Because of the cumulative effect, if the Battery Power Scheme timers are set to 3 seconds, 15 seconds and 5 minutes:

- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15 sec + 3 sec),
- And the device enters Suspend after 5 minutes and 18 seconds of no activity.

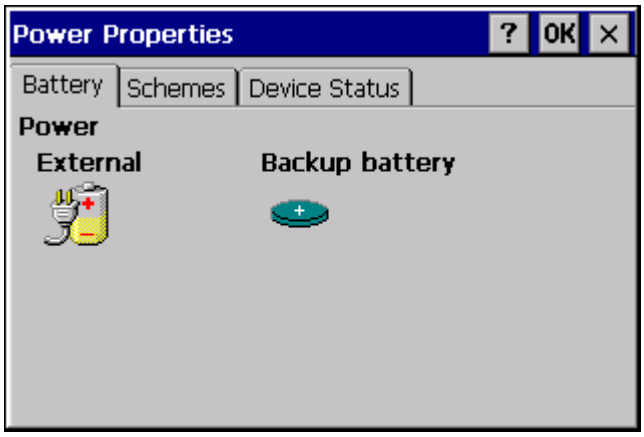
If the User Idle timer is set to Never, the power scheme timers never place the device in User Idle, System Idle or Suspend modes.

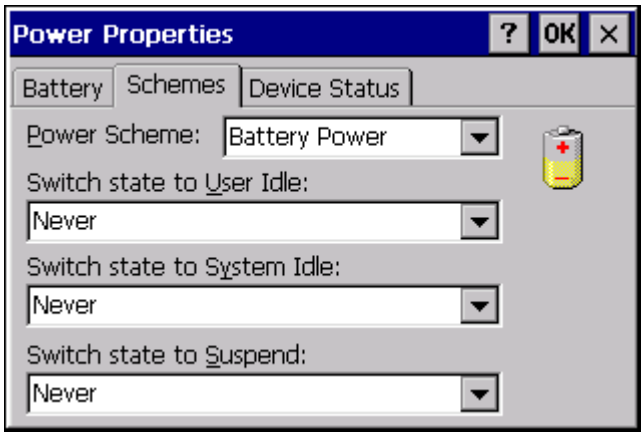
The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the count-down after the System Idle timer has expired.

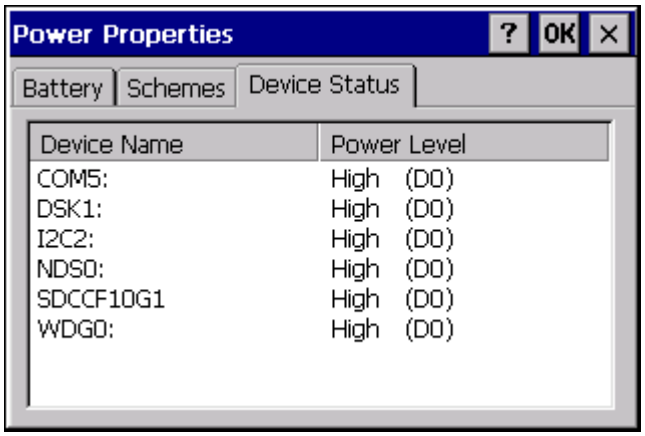
When the User Idle timer is set to “Never”, the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

The **Display > Backlight** setting is synchronized with the User Idle setting in the Schemes tab in the Power control panel.

Setting	Default
Battery tab	
Schemes tab	
Battery Power - User Idle Timeout	Never
Battery Power - System Idle Timeout	Never
Battery Power - Suspend Timeout	Never
AC Power - User Idle Timeout	Never
AC Power - System Idle Timeout	Never
AC Power - Suspend Timeout	Never
Device Status tab	No user interaction





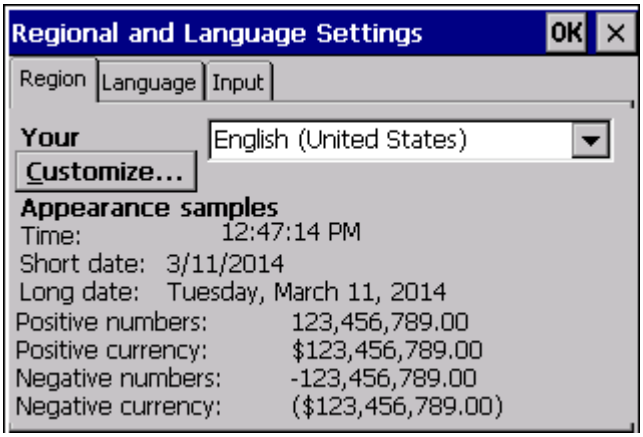

Power Properties
?
OK
Battery
Schemes
Device Status
Device Name
Power Level
COM5:
High (D0)
DSK1:
High (D0)
I2C2:
High (D0)
NDS0:
High (D0)
SDCCF10G1
High (D0)
WDG0:
High (D0)

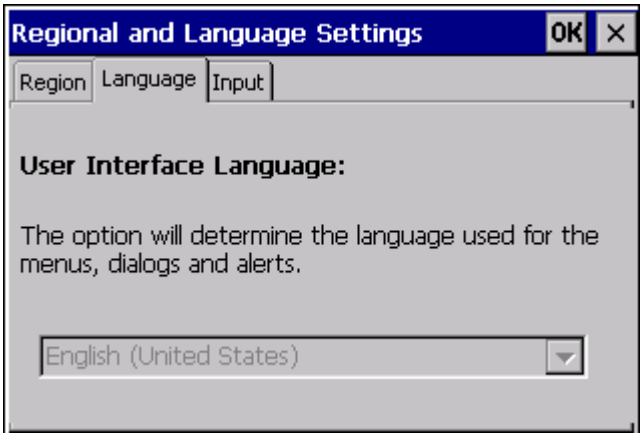
Regional and Language Settings

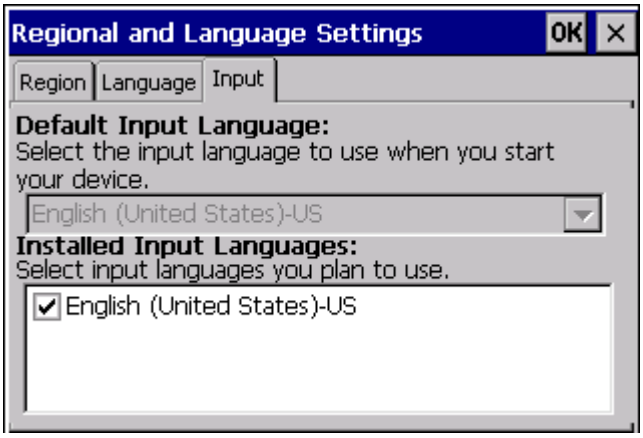
Start > Settings > Control Panel > Regional Settings

Set the appearance of numbers, currency, time and date based on regional and language settings. Set the HX3 user interface language and the default input language.

Setting	Default
Region	
Locale	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	$123,456,789.00 pos / ($123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long
Language	
User Interface	English (United States)
Input	
Language	English (United States)-US
Installed	English (United States)-US







Remove Programs

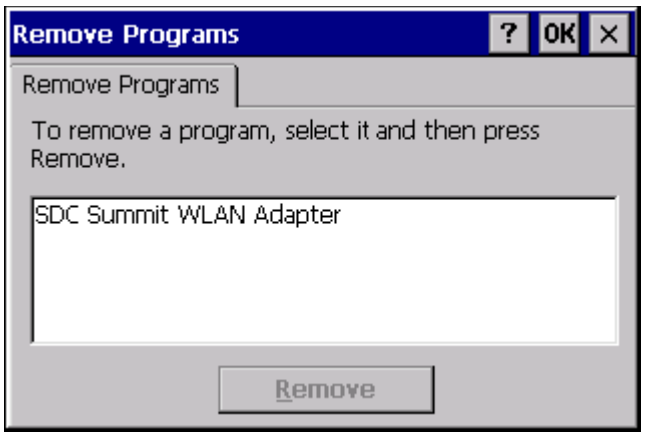
Start > Settings > Control Panel > Remove Programs

Note: Lists programs installed in RAM that have been marked for removal.

In some OS versions, this panel is replaced by the Installed Programs panel. The Installed Programs panel does not allow any user interaction.

Select a program and tap Remove. Follow the prompts on the screen to uninstall HX3 user-installed only programs. The change takes effect immediately.

Files stored in the My Documents folder are not removed using this option.



Note: Do not remove installed programs using this option. Contact Customer Support (page 14-1) if installed programs must be deleted.

System

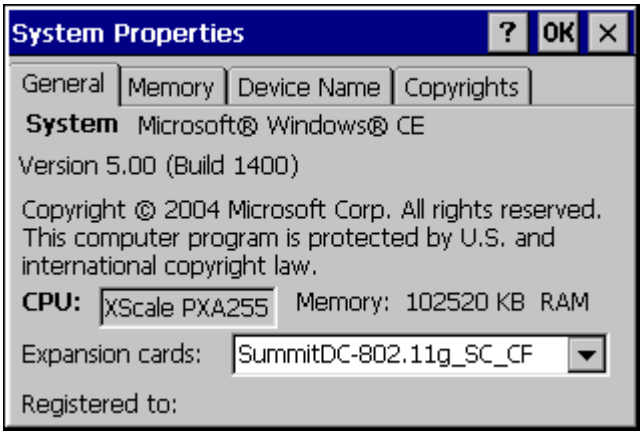
Start > Settings > Control Panel > System

Use these HX3 panels to:

- Review System and mobile device data and revision levels.
- Adjust Storage and Program memory settings.
- Assign a device name and device descriptor.

Setting	Default
General	No user interaction
Memory	1/3 storage, 2/3 program memory
Device Name and Description	Unique to equipment type
Copyrights	No user interaction

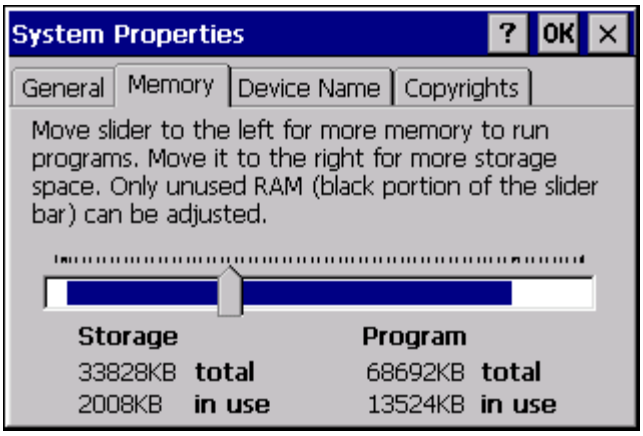
General Tab



System: This screen is presented for information only. The System parameters cannot be changed by the user.

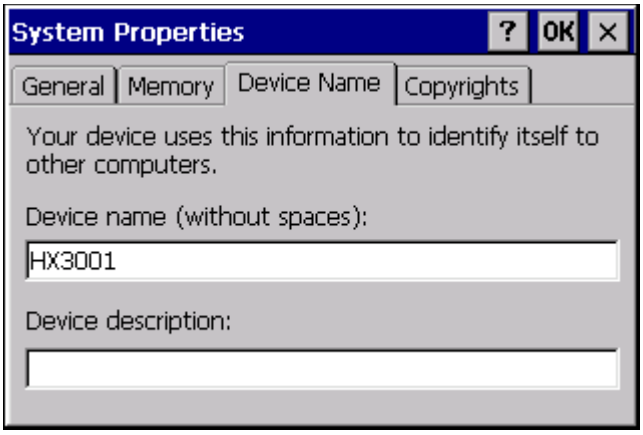
Computer: The processor type is listed. The type cannot be changed by the user. Total computer memory and the identification of the registered user is listed and cannot be changed by the user. Memory sizes given do not include memory used up by the operating system. For example, a system with 128 MB may only report 99 MB memory, since 29 MB is used by the operating system. This is actual DRAM memory, and does not include internal flash used for storage.

Memory Tab



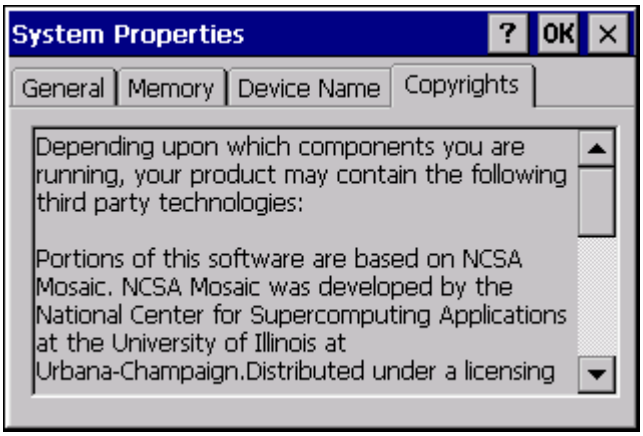
Move the slider to allocate more memory for programs or storage. If there isn't enough space for a file, increase the amount of storage memory. If the mobile device is running slowly, try increasing the amount of program memory.

Device Name Tab



The device name and description can be changed by the user. Enter the name and description using either the keypad or the Input Panel and tap OK to save the changes. This information is used to identify the HX3 to other computers and devices.

Copyrights Tab



This screen is presented for information only. The Copyrights information cannot be changed by the user.

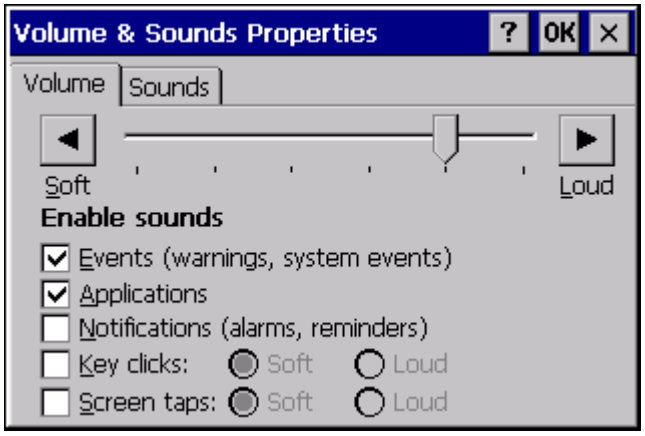
Volume and Sounds

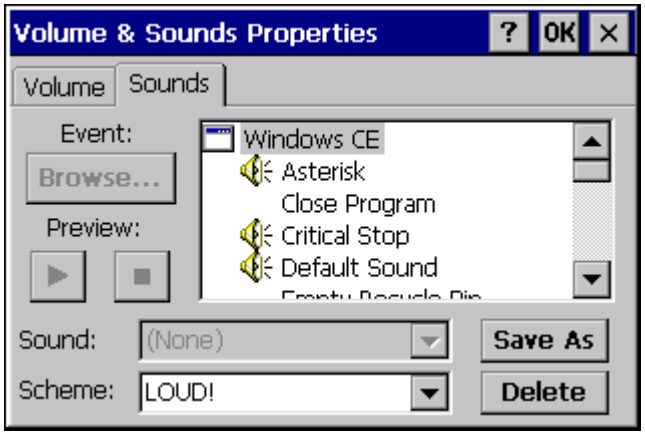
Start > Settings > Control Panel > Volume & Sounds

Note: An application may override the control of the speaker volume. Turning off sounds saves power and prolongs battery life.

Set volume parameters and assign sound WAV files to CE events using these options. You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft. As the volume scrollbar is moved between Loud and Soft, the HX3 emits a tone each time the volume increases or decreases. Volume must be enabled when you want to adjust volume settings using keypad keys.

Setting	Default
Volume	
Events	Enabled
Application	Enabled
Notifications	Disabled
Volume	Middle of Bar
Key click	Disabled
Screen tap	Disabled
Sounds	
Scheme	LOUD!





The volume setting is stored in the registry and is recalled at power on.

Rejected bar codes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from a tethered scanner, and then the rejection of scanned bar code data by the bar code processing causes a bad scan beep from the mobile device on the same data.

Good Scan and Bad Scan Sounds

Good scan and bad scan sounds are stored in the Windows directory, as SCANGOOD.WAV and SCANBAD.WAV. These are unprotected WAV files and can be replaced by a WAV file of the user's choice.

By default a good scan sound on the HX3 is a single beep, and a bad scan sound is a double beep.

Wi-Fi

Start > Settings > Control Panel > Wi-Fi or click the Summit Client Utility icon

Use this option to set parameters and manage profiles for the HX3 wireless client.

See Summit Client Utility (page 9-1) for information and instruction.

6

Bluetooth Configuration

Introduction

Before any software configuration can occur, the HX3 must be connected to a host computer with a USB port. The HX3 does not have a touch screen. Because of this and the limited keypad, it is necessary to configure the HX3 using ActiveSync and LXEConnect.

Note: The HX3 does not have a touch screen. If the host computer has a touch screen, instructions using "tap" and "stylus" instead of "click" and "mouse" apply. Discover and manage pairing with nearby Bluetooth devices.

Due to the headless design of the HX3, all Bluetooth dialog pop-up boxes are suppressed by default, even when the HX3 is viewed with LXEConnect. The dialog pop-ups may be enabled for viewing with a remote management tool such as LXEConnect. However, to preserve battery life, the dialog pop-ups should be turned off when the HX3 is not being viewed with a remote management utility.

Setting	**Default**
Discovered Devices	None
Settings	
Turn off Bluetooth	Enabled
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Disabled
Continuous search	Enabled
Filtered Mode	Enabled
Printer Port on COM 9:	Disabled (unchecked) by default in both Filtered and Non Filtered Modes. The option is dimmed in Non Filtered Mode.
Logging	Disabled
Computer Friendly Name	System Device Name
Reconnect	
Report lost connection	Disabled
Report when reconnected	Disabled
Report failure to reonnect	Disabled
Clear Pairing Table on boot	Disabled
Auto Reconnect on Boot	Enabled
Auto Reconnect	Enabled
OPP Setup	
Inbox	\My Device\My Documents\DefaultInbox
Outbox	\My Device\My Documents\DefaultOutbox
Write Capable	Enabled
Enable Notifications	Enabled
Disable LXEZ Pairing OPP	Unchecked, OPP is enabled

Bluetooth taskbar Icon state and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the HX3.

The default Bluetooth setting is On.

The HX3 cannot be discovered by other Bluetooth devices when the Computer is discoverable option is disabled (unchecked) on the Settings panel.

Other Bluetooth devices cannot be discovered if they have been set up to be Non-Discoverable or Invisible.

- When Filtered Mode is enabled, the HX3 can pair with one Bluetooth scanner and one Bluetooth printer.
- When Filtered Mode is disabled, the HX3 can pair with up to four Bluetooth devices, with a limit of one scanner, one printer, two HID devices (one Mouse, one Keyboard), one PAN device, and one DUN device connected at the same time.
- It is not necessary to disconnect a paired scanner and printer before a different scanner or printer is paired with the HX3.
- The target Bluetooth device should be as close as possible (up to 32.8 ft (10 meters) Line of Sight) to the HX3 during the pairing process.

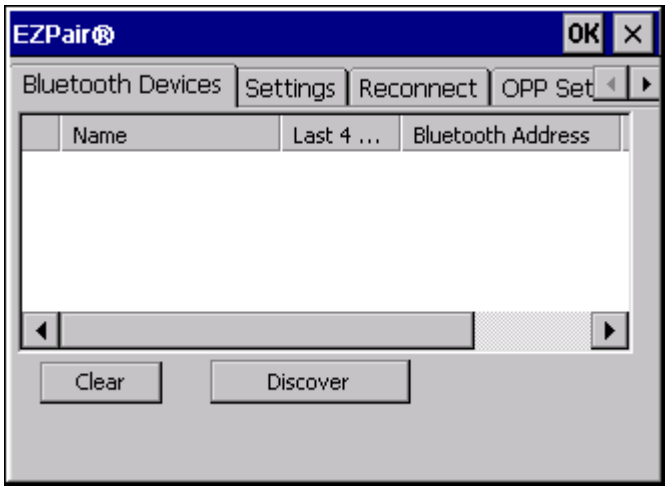
Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the HX3. The HX3 operating system has been upgraded to the revision level required for Bluetooth client operation. An application (or API) is available that will accept data from serial Bluetooth devices.

HID	Human Interface Device	HID profiles used by Bluetooth keyboards, mice, pointing devices and remote monitoring devices.
PAN	Personal Area Networking	PAN profiles, unmodified Ethernet payloads (using BNEP) can exchange packets between Bluetooth devices. PANU is a PAN User service that uses either the NAP or the GN service.
DUN	Dial-Up Networking	DUN provides access to the Internet and other dial-up services using Bluetooth technology.

Bluetooth Devices Panel

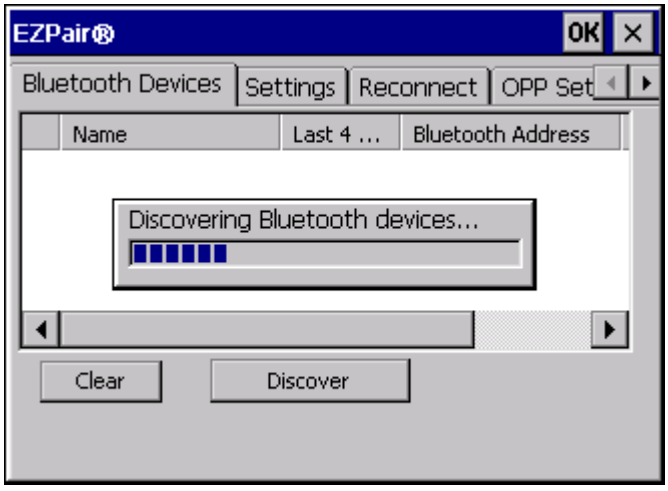
Note: The HX3 does not have a touch screen. If the host computer has a touch screen, instructions using "tap" and "stylus" instead of "click" and "mouse" apply.

Note: The Bluetooth Devices tab displays any device previously discovered and paired with the HX3.



Discover

Tap the Discover button to locate all discoverable Bluetooth devices in the vicinity. The Discovery process also queries for the unique identifier of each device discovered.

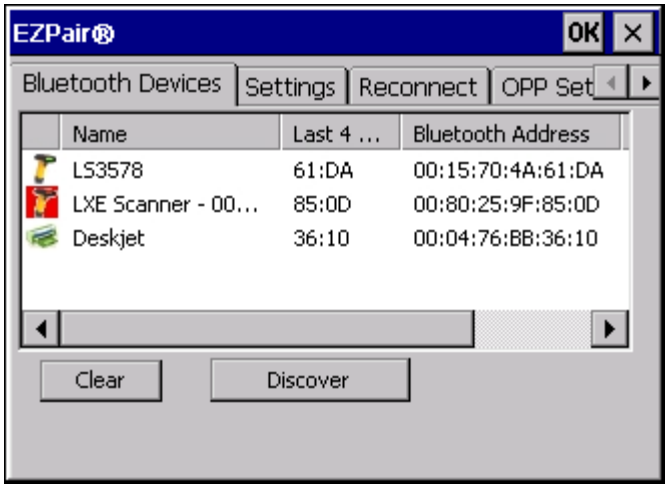


Stop Button

Tap Stop at any time to end the Discover and Query for Unique Identifier functions. Devices not paired are not shown after any reboot sequence.

When an active paired device enters Suspend Mode, is turned Off or leaves the HX3 Bluetooth scanning range, the Bluetooth connection between the paired device and the HX3 is lost. There may be audible or visual signals as paired devices disconnect from the HX3.

Bluetooth Device List



The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as a Scanner or a Printer. The Bluetooth panel assigns an icon to the device name.

The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as a Serial device, a Bluetooth scanner, a Bluetooth printer, a PAN, and a DUN connected at the same time. More than one HID device can be connected but only one Bluetooth mouse and one Bluetooth keyboard. The Bluetooth panel assigns an icon to the device name.

An icon with a red background indicates the device's Bluetooth connection is inactive.

An icon with a white background indicates the device is connected to the HX3 and the device's Bluetooth connection is active.

Double-tap a device in the list to open the device properties menu. The target device does not need to be active.

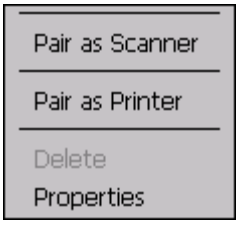
Clear Button

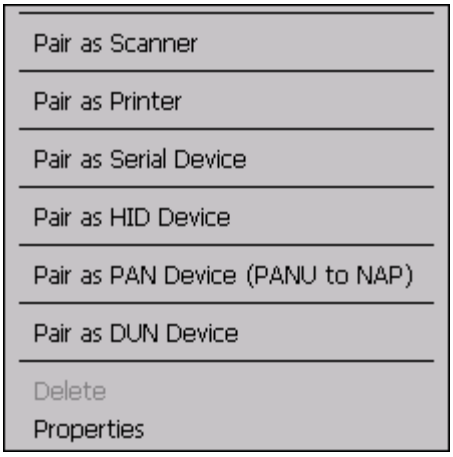
Deletes all devices from the Device table that are not currently paired. A dialog box is presented, “Delete all disconnected devices? Yes/No”. Tap the Yes button to remove disconnected or deleted devices from the device table. The devices are removed from the Device table after any reboot sequence or after closing and reopening the Bluetooth panels. Tap the No button to make no changes.

Bluetooth Device Menu

Pre-requisite: The Discover button has been clicked and there are Bluetooth devices listed.

Click on a device in the list to highlight it. Double click the highlighted device to display the Bluetooth Device right click menu. The Bluetooth device does not need to be active.





Filtered Mode Enabled Filtered Mode Disabled

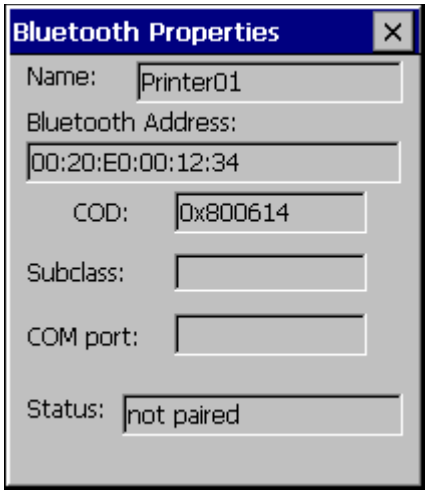
Right Click Menu Options

Pair as Scanner	Receive data from the highlighted Bluetooth scanner or Bluetooth imager.
Pair as Printer	Send data to the highlighted Bluetooth printer.
Pair as Serial Device	Communicate with the highlighted serial Bluetooth device. This option is available when Filtered Mode is disabled.
Pair as HID Device	Communicate with the highlighted HID (Human Interface Device). This option is available when Filtered Mode is disabled/unchecked.
Pair as PAN Device (PANU to NAP)	Communicate with the highlighted PAN (Personal Area Networking) device. This option is available when Filtered Mode is disabled/unchecked.
Pair as DUN Device	Communicate with the highlighted DUN (Dial-Up Networking) device. This option is available when Filtered Mode is disabled/unchecked.
Disconnect	Stop the connection between the HX3 and the highlighted paired Bluetooth device.
Delete	Remove an unpaired device from the Bluetooth device list. The highlighted device name and identifier is removed from the HX3 Bluetooth Devices panel after the user taps OK.
Properties	More information on the highlighted Bluetooth device.

Bluetooth Properties Panel

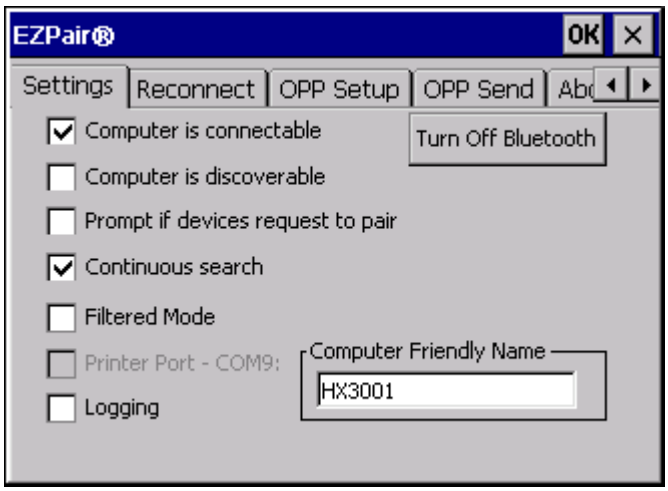
Data on the Bluetooth Properties panel cannot be changed by the user. The data displayed is the result of the device Query performed during the Discovery process.

The Status dialog box reflects the current state of the highlighted device.



Settings Panel

Due to the headless design of the HX3, all Bluetooth dialog pop-up boxes are suppressed by default, even when the HX3 is viewed with LXEConnect. The dialog pop-ups may be enabled for viewing with a remote management tool such as LXE-Connect. However, to preserve battery life, the dialog pop-ups should be turned off when the HX3 is not being viewed with a remote management utility.



These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

Turn Off Bluetooth (Button)

Tap the button to toggle the Bluetooth client On or Off. The button title changes from Turn Off Bluetooth to Turn On Bluetooth.

The default value is Bluetooth On.

Settings

Computer is connectable

This option is Enabled by default. Disable this option to inhibit HX3 connection initiated by a Bluetooth scanner.

Computer is discoverable

This option is Disabled by default. Enable this option to ensure other devices can discover the HX3.

Prompt if devices request to pair

This option is Disabled by default. A dialog box appears on the HX3 screen notifying the user a Bluetooth device requests to pair with the HX3. The requesting Bluetooth device does not need to have been Discovered by the HX3 before the pairing request is received. Tap the Accept button or the Decline button to remove the dialog box from the screen.

In some cases, if a Bluetooth device is already paired this setting cannot be changed. If this is the case, an error message is displayed and the option is not changed. The Bluetooth device must be disconnected before changing this setting.

Continuous Search

This option is Enabled by default. When enabled, the Bluetooth connection never stops searching for a device it has paired with when the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the HX3 stops searching after 30 minutes.

This option draws power from the Main Battery.

Filtered Mode

This option is Enabled by default. Determines whether the Bluetooth client discovers and displays all serial Bluetooth devices in the vicinity (Filtered Mode is disabled/unchecked) or the discovery result displays Bluetooth scanners and printers only (Filtered Mode is enabled/checked). When Filtered Mode is disabled, the HX3 can pair with up to four Bluetooth devices, with a limit of one Bluetooth scanner, one Bluetooth printer, one PAN, and one DUN connected at the same time. More than one HID device can be connected but only one Bluetooth mouse and one Bluetooth keyboard.

A Warmboot is required every time Filtered Mode is toggled on and off.

Printer Port - COM9

This option is Disabled by default. This option assigns Bluetooth printer connection to COM9 instead of COM19. To enable this option, Filtered Mode must be enabled.

Logging

This option is Disabled by default. When logging is enabled, the HX3 creates bt_log.txt and stores it in the /System folder. Bluetooth activity logging is added to the text file as activity progresses. A bt_log_bak.txt file contains the data stored by bt_log.txt prior to reboot. During a reboot process, the HX3 renames bt_log.txt to bt_log_bak.txt. If a file already exists with that name, the existing file is deleted, the new bt_log_bak.txt file is added and a new bt_log.txt is created.

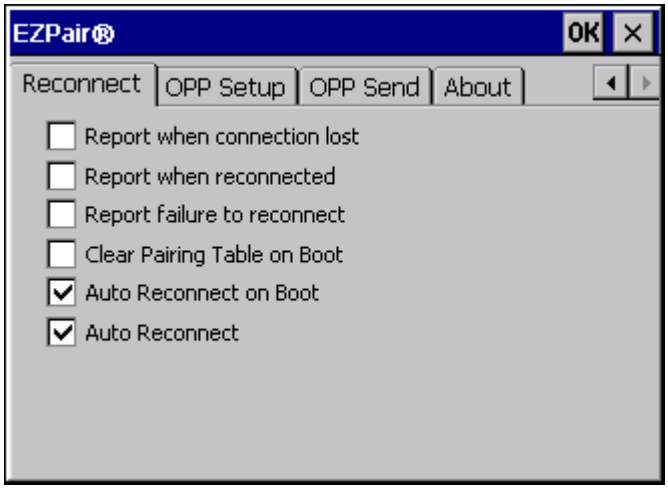
Computer Friendly Name

Default: Computer System Name (**System Panel > Device Name** tab).

The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.

Reconnect Panel

Due to the headless design of the HX3, all Bluetooth dialog pop-up boxes are suppressed by default, even when the HX3 is viewed with LXEConnect. The dialog pop-ups may be enabled for viewing with a remote management tool such as LXE-Connect. However, to preserve battery life, the dialog pop-ups should be turned off when the HX3 is not being viewed with a remote management utility.



Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

Settings

Report when connection lost

This option is Disabled by default. There may be an audio or visual signal when a connection between a paired, active device is lost. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. Tap the ok button to remove the dialog box from the screen.

Report when reconnected

This option is Disabled (unchecked) by default. There may be an audio or visual signal when a connection between a paired, active device is made. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has resumed. Tap the ok button to remove the dialog box from the screen.

Report failure to reconnect

This option is Disabled by default. The default time delay is 30 minutes. This value cannot be changed by the user. There may be an audio or visual signal when a connection between a paired, active device fails to re-connect. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the previously paired Bluetooth devices has failed. Tap the X button or ok button to close the dialog box. Possible reasons for failure to reconnect: Timeout expired without reconnecting; attempted to pair with a device that is currently paired with another device; attempted to pair with a known device that moved out of range or was turned off; attempted to pair with a known device but the reason why reconnect failed is unknown.

Clear Pairing Table on Boot

This option is Disabled (unchecked) by default. When enabled (checked), all previous paired information is deleted upon any reboot sequence and no devices are reconnected. When enabled (checked) “Auto Reconnect on Boot” is automatically disabled (dimmed).

Auto Reconnect on Boot

This option is Enabled (checked) by default. All previously paired devices are reconnected upon any reboot sequence. When disabled (unchecked), no devices are reconnected upon any reboot sequence.

Auto Reconnect

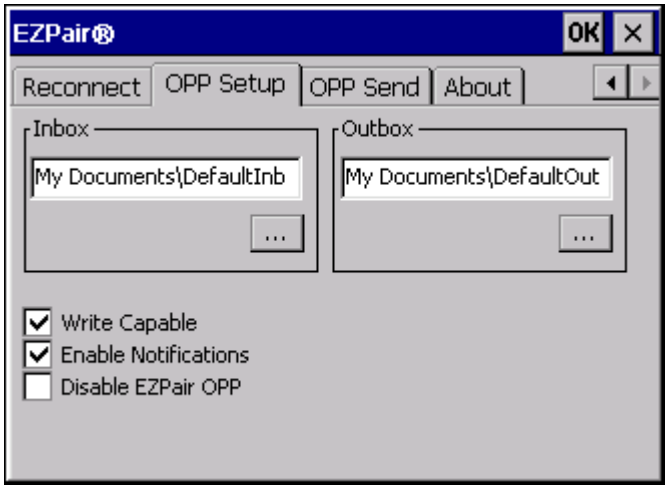
This option is Enabled (checked) by default. This option controls the overall mobile Bluetooth device reconnect behavior.

When Auto Reconnect is disabled (unchecked), Auto Reconnect on Boot is automatically disabled and dimmed.

- When Auto Reconnect is disabled (unchecked), no devices are reconnected in any situation. The status of Auto Reconnect on Boot is ignored and no devices are reconnected on boot. The status of Clear Pairing Table on Boot controls whether the pairing table is populated on boot.
- When Auto Reconnect is enabled (checked) and Auto Reconnect on Boot is disabled (unchecked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range).
- When Auto Reconnect is enabled (checked) and Clear Pairing Table on Boot is enabled (checked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). The pairing table is cleared on boot. The status of Auto Reconnect on Boot is ignored and the option is automatically disabled (unchecked) and dimmed.

OPP Setup Panel

Use this screen to setup the HX3 for Object Push Protocol (OPP).



Inbox

This is an alphanumeric field displaying the currently selected Inbox.

The Inbox is the location where files pushed to the HX3 from a remote client are stored. Use the browse button ... to browse to and select the Inbox folder.

Use Windows Explorer to create a custom directory, if desired, before selecting the Inbox folder.

- The default Inbox is \My Device\My Documents\DefaultInbox.

Outbox

This is an alphanumeric field displaying the currently selected Outbox.

The Outbox is the location where files are stored to be pushed from the HX3 to a remote server. Use the browse button ... to browse to and select the Outbox folder.

Use WExplorer to create a custom directory, if desired, before selecting the Outbox folder.

- The default Inbox is \My Device\My Documents\DefaultOutbox.

Write Capable

When checked, files may be written to the HX3. When unchecked, inbound files are rejected. This option is enabled (checked) by default.

Enable Notifications

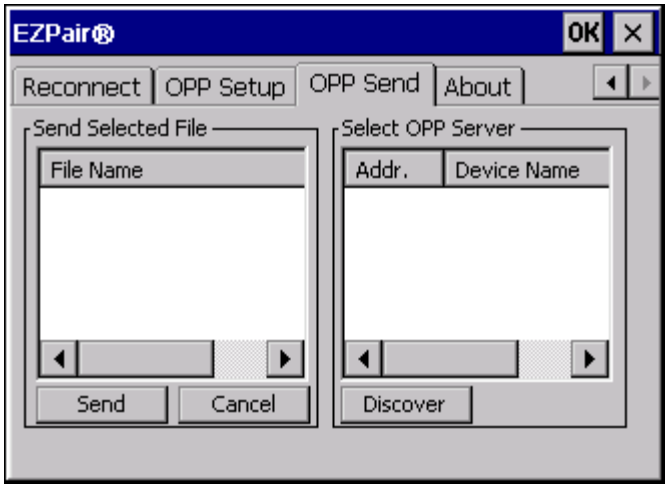
When checked, the user is notified and may be prompted for a response when files are received by the HX3. When unchecked, inbound files are received with no notification to and no required action from the user. This option is enabled (checked) by default.

Disable LXEZ Pairing OPP

When checked, OPP is disabled in LXEZ Pairing. When unchecked, OPP is enabled in LXEZ Pairing. The default is unchecked, OPP is enabled for LXEZ Pairing.

- Because only one application can use OPP at a given time, custom applications should disable OPP in LXEZ Pairing via an API call while the application is using OPP and restore this setting upon completion.
- When this item is checked, the other parameter settings on this screen are unavailable (dimmed).

OPP Send Panel



If LXEZ Pairing OPP is disabled, no file names or OPP servers are displayed on this tab. These areas are grayed out. Similarly the buttons on this tab are also inactive when LXEZ Pairing OPP is disabled.

Send Selected File From Outbox

This area displays the file listing from the currently selected Outbox. All files are shown (*.*). The most recently pushed file is highlighted, assuming that file is still present in the Outbox.

Select OPP Server from Remote Device List

This list displays the known OPP capable servers that the HX3 has previously discovered. The most recently paired server is selected and highlighted.

Buttons

Send - Tapping this button sends (pushes) the selected file to the remote (server) device.

Cancel - Tapping this button cancels the send process initiated by tapping the Send button.

Discover - Tapping this button initiates a discovery of OPP devices. Results of the discovery are shown in the OPP Server selection box.

About Panel

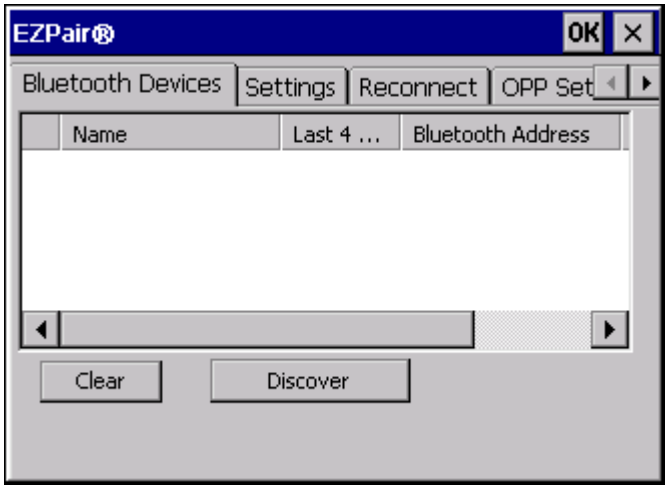
This panel lists the assigned Computer Friendly Name (that other devices may discover during their Discovery and Query process), the Bluetooth MAC address, and software version levels. The data cannot be edited by the user.

Using Bluetooth

The HX3 default Bluetooth setting is Enabled. The HX3 Bluetooth® module is designed to Discover and pair with nearby Bluetooth devices.

Prerequisite: The Bluetooth devices have been setup to allow them to be “Discovered” and “Connected/Paired”. The System Administrator is familiar with the pairing function of the Bluetooth devices.

Bluetooth Devices Display - Before Discovering Devices



When Filtered Mode is enabled, only LXE Bluetooth printers or Bluetooth scanners/imagers are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.

Initial Configuration

1. Select **Start > Settings > Control Panel > Bluetooth** or tap the Bluetooth icon in the taskbar or on the desktop.
2. Tap the Settings Tab.
3. Change the Computer Friendly Name at the bottom of the Settings display. The Bluetooth HX3 default name is determined by the factory installed software version. Honeywell strongly urges assigning every HX3 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Check or uncheck the HX3 Bluetooth options on the Settings and Reconnect tabs.
5. Tap the OK button to save your changes or the X button to discard any changes.

Subsequent Use

Taskbar and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. A taskbar Bluetooth icon with a red background indicates Bluetooth is active and not paired with any device. A device icon with a red background indicates a disconnected paired device.

1. Tap the Bluetooth icon in the taskbar or on the desktop to open the Bluetooth LXEZ Pairing application.
2. Tap the Bluetooth Devices tab.
3. Tap the Discover button. When the Bluetooth module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
4. The discovered devices are listed in the Bluetooth Devices window.
5. Highlight a Bluetooth device in the Discovered window and double-tap to open the device properties menu.
6. Tap Pair as Scanner to set up the HX3 to receive scanner data.
7. Tap Pair as Printer to set up the HX3 to send data to the printer.
8. Tap Serial Device (when Filtered mode is disabled) to set up the HX3 to communicate with a Bluetooth serial device.
9. Tap HID Device to pair a Human Interface device.
10. Tap PAN Device to pair a Personal Area Networking device.
11. Tap DUN Device to pair a Dial-Up Networking device.
12. Tap Disconnect to stop pairing with the device. Once disconnected, tap Delete to remove the device name and data from the HX3 Bluetooth Devices list. The device is deleted from the list after the OK button is clicked.
13. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the HX3 display.
14. Whenever the HX3 is turned On, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the HX3. If the devices cannot connect to the HX3 before the re-connect timeout time period expires (default is approximately 20 seconds for each paired device) there is no indication of the continuing disconnect state if Report Failure to Reconnect is disabled.

Bluetooth Indicators

The Bluetooth taskbar Icon state and Bluetooth LED state change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the HX3.

Taskbar Icon	Legend
	HX3 is connected to one or more of the targeted Bluetooth device(s).
	HX3 is not connected to any Bluetooth device. HX3 is ready to connect with any Bluetooth device. HX3 is out of range of all paired Bluetooth device(s). Connection is inactive.

When an active paired device enters Suspend Mode, is turned Off or leaves the HX3 Bluetooth scan range, the Bluetooth connection between the paired device and the HX3 is lost. There may be audible or visual signals as paired devices disconnect from the HX3.

Bluetooth LED	Legend
Blue, blinking slowly	Bluetooth is active but not connected to a device.
Blue, blinking medium	Bluetooth is paired and connected to a device.
Blue, blinking fast	Bluetooth is discovering other Bluetooth devices.
Off	Bluetooth hardware has been turned off or does not exist in the HX3.

Bluetooth Bar Code Reader Setup

Refer to the Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site. Several different types of bar code readers are supported. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the HX3 using Bluetooth functions.

Prerequisites

- The HX3 has the Bluetooth hardware and software installed. An operating system upgrade may be required.
- If the HX3 has a Bluetooth address identifier bar code label affixed, then Bluetooth hardware and software is installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The HX3 main battery is fully charged. Alternatively, the HX3 may be in a powered cradle or cabled to AC/DC power.
- Important: The bar code numbering examples in this segment are not real and should not be created or scanned with a Bluetooth scanner.
- To open the LXEZ Pairing program, tap **Start > Settings > Control Panel > Bluetooth** or tap the Bluetooth icon on the desktop or tap the Bluetooth icon in the taskbar.

Locate the bar code label, similar to the one shown above, attached to the HX3. The label is the Bluetooth address identifier for the HX3.

The mobile Bluetooth scanner / imager requires this information before discovering, pairing, connecting or disconnecting can occur.

Important: The HX3 Bluetooth address identifier label should remain protected from damage (rips, tears, spills, soiling, erasure, etc.) at all times. It may be required when pairing, connecting, and disconnecting new Bluetooth bar code readers.

HX3 with Label

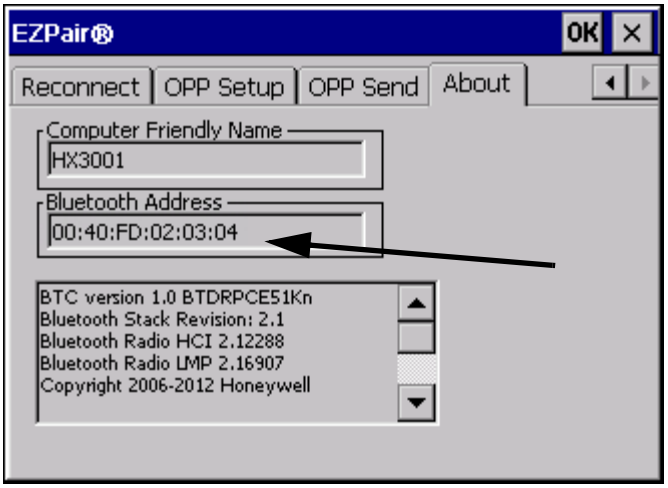
If the HX3 has a Bluetooth address bar code label attached, follow these steps:

1. Scan the Bluetooth address bar code label, attached to the HX3, with the Bluetooth mobile scanner.
2. If this is the first time the Bluetooth mobile scanner has scanned the HX3 Bluetooth label, the devices are paired. If the devices do not pair successfully, go to the next step.
3. Open the LXEZ Pairing panel (**Start > Settings > Control Panel > Bluetooth**).
4. Tap Discover. Locate the Bluetooth scanner in the Discovery panel.
5. Double-tap the stylus on the Bluetooth mobile device in the list. The right-mouse-click menu appears.
6. Select Pair as Scanner to pair the HX3 with the Bluetooth mobile scanner.
7. The devices are paired. The Bluetooth mobile bar code reader responds with a series of beeps and an LED flashes.
8. After scanning the HX3 Bluetooth label, if there is no beep and no LED flash from the Bluetooth mobile device, the devices are currently paired.

HX3 without Label

If the HX3 Bluetooth address bar code label does not exist, follow these steps to create a unique Bluetooth address bar code for the HX3:

First, locate the HX3 Bluetooth address by tapping **Start > Settings > Control Panel > Bluetooth > About** tab.



Next, create a Bluetooth address bar code label for the HX3. Free bar code creation software is available for download on the World Wide Web. Search using the keywords “bar code create”.

The format for the bar code label is as follows:

- Bar code type must be Code 128.
- FNC3 character followed by string Uppercase L, lowercase n, lowercase k, uppercase B and then the Bluetooth address (12 hex digits, no colons). For example, LnkB0400fd002031.

Create and print the label.

Scan the HX3 Bluetooth address bar code label with the Bluetooth bar code reader.

The devices are paired. The Bluetooth bar code reader responds with a series of beeps and LED flashes.

After scanning the HX3 Bluetooth label, if there is no beep and no LED flash from the Bluetooth bar code reader, the devices are currently paired.

Bluetooth Beep and LED Indications

Paired External Bluetooth Device

Beep Type from Bluetooth Device	Behavior
Acknowledge label	1 beep
Label rejected	2 beeps at low frequency
Transmission error	Beep will sound high-low-high-low
Link successful	Beep will sound low-medium-high
Link unsuccessful	Beep will sound high-low-high-low

Paired External Bluetooth Device

LED on Bluetooth Device	Behavior
Yellow LED blinks at 2 Hz	Linking in progress
Off	Disconnected or unlinked
Yellow LED blinks at 50 Hz	Bluetooth transmission in progress
Yellow LED blinks at the same rate as the paging beep (1 Hz)	Paging
Green LED blinks once a second	Disabled indication

Upon startup, if the mobile Bluetooth scanner sounds a long tone, this means the scanner has not passed its automatic Selftest and has entered isolation mode. If the scanner is reset, the sequence is repeated. Contact Customer Support (page 14-1) for help with external Bluetooth devices.

Bluetooth Printer Setup

The Bluetooth managed device should be as close as possible, in direct line of sight, with the HX3 during the pairing process.

1. Open the LXEZ Pairing Panel.
2. Tap Discover. Locate the Bluetooth printer in the Discovery panel.
3. Tap and hold the stylus (or doubletap) on the Bluetooth printer ID until the right-mouse-click menu appears.
4. Select Pair as Printer to pair the HX3 with the Bluetooth managed printer.

The devices are paired. The Bluetooth managed printer may respond with a series of beeps or LED flashes.

Refer to the Bluetooth managed printer manufacturer's User Guide; it may be available on the manufacturer's web site. Contact Customer Support (page 14-1) for Bluetooth product assistance.

If there is no beep or no LED flash from the Bluetooth managed printer, the HX3 and the printer are currently paired.

Easy Pairing and Auto-Reconnect

The Bluetooth module can establish relationships with new devices after the user taps the Discover button. It can auto-reconnect to devices previously known but which have gone out of range and then returned within range.

Configuration elements are persistent and stored in the registry.

Setup the Bluetooth module to establish how the user is notified by easy pairing and auto-reconnect events.

Using OPP

Pairing with an OPP Device

Prerequisites

- A remote device, such as a mobile phone, that supports OPP.
- OPP is enabled on the HX3.

1. Place the remote device in discovery or visible mode.
2. Initiate discovery on the HX3 by tapping the Discover button on the OPP Send tab.
3. The HX3 discovers the remote device.
4. The HX3 attempts to send a file to the remote device.
5. The remote device prompts the user for a 4 digit PIN.
6. User enters the PIN.
7. The HX3 prompts the user for a 4 digit PIN.
8. User must enter the *same* PIN code as entered on the remote device.
9. The HX3 now pairs with the remote device.

Remote Device Pushes File to HX3

This section assumes that a device supporting OPP is paired with the HX3.

If a duplicate filename is received, LXEZ Pairing writes the file in the specified location, with an incremental number appended to the file name. For example, if a file named file.jpg is pushed to the HX3 and that filename already exists in the Inbox, LXEZ Pairing saves the new file as file001.jpg. If the same file is pushed again, it is saved as file002.jpg.

There are several scenarios based on configuration options on the OPP Setup tab.

Notifications enabled, HX3 **is Write Capable**

1. The OPP client initiates a connection to the HX3 by selecting a file to push to the HX3.
2. The HX3 user is notified that a File Push request has been issued from a remote device.
3. The HX3 user is prompted to accept or reject the incoming request.
4. If the user accepts the request:
   - The file is pushed to the HX3.
   - LXEZ Pairing notifies the user that a file has been received.
   - The connection is closed by the remote device (OPP client).
5. If the user rejects the request:
   - The file is not pushed to the HX3.
   - The connection is closed.

Notifications enabled, HX3 **is not Write Capable**

1. The OPP client initiates a connection to the HX3 by selecting a file to push to the HX3.
2. The file is rejected silently (no notification to the HX3 user).

Notifications disabled, HX3 **is Write Capable**

1. The OPP client initiates a connection to the HX3 by selecting a file to push to the HX3.
2. The file is accepted silently (no notification to the HX3 user).

Notifications disabled, HX3 **is not Write Capable**

1. The OPP client initiates a connection to the HX3 by selecting a file to push to the HX3.
2. The file is rejected silently (no notification to the HX3 user).

HX3 Pushes File to Remote Device

This section assumes that a device supporting OPP is paired with the HX3.

The HX3 (OPP client) initiates a connection to the remote device (OPP server) by selecting a file to push to the remote device. The HX3 sends the file and disconnects. The remote device may prompt the user (of that remote device) to accept the incoming request depending on the security settings of the remote device. The prompt may be displayed more than once, or it may not be displayed at all.

Notifications enabled

The file is pushed to the remote device and the user of the HX3 is notified of the completion of the push.

Notifications disabled

The file is pushed to the remote device and the user of the HX3 is not notified of the completion of the push.

LXEZ Pairing and External Application

Because only one application can use the OPP service at a time, external applications that wish to use OPP should disable LXEZ Pairing OPP before using the OPP service and restore LXEZ Pairing OPP upon completion using available API calls (see the *CE API Programming Guide* for details). These API calls are the equivalent of checking or unchecking the Disable LXEZ Pairing OPP check box.

- If Disable LXEZ Pairing OPP is not checked, checking it causes LXEZ Pairing OPP to be disabled and the send and receive functionality is disabled.
- If Disable LXEZ Pairing OPP is checked, and no application has registered a callback, un-checking LXEZ Pairing OPP enables OPP functionality in LXEZ Pairing, and the send and receive functionality is enabled.
- If Disable LXEZ Pairing OPP is checked, and another application has registered a callback, un-checking Disable LXEZ Pairing OPP issues a dialog box which says “Another application is using OPP. Do you wish to force their disconnection? Doing so will force the other application to be unregistered.” The application that has been forcibly unregistered receives a FORCED_UNREGISTER_RECEIVED event.

7 Bar Code Scanner Wedge

Introduction

Set HX3 scanner keyboard wedge parameters, enable or disable allowed symbologies, scanner icon appearance, active scanner port, and scan key settings. Assign baud rate, parity, stop bits and data bits for available COM ports.

The HX3 does not have a touch screen. If the host computer has a touch screen, instructions using “tap” and “stylus” instead of “click” and “mouse” apply.

Bar code manipulation parameter settings on the Barcode tab are applied to the incoming data resulting from successful bar code scans sent to the HX3 for processing. The successful bar code scan data may be sent by

a wireless Bluetooth hand-held Scanner,

or a tethered ring scanner / imager.

- After hot swapping HX3 ring scanners, the HX3 auto-detects the ring scanner type. The decoder engine activates when the Scan button on the ring is pressed.

Bar Code Readers

Your HX3 may have any of the following body worn bar code readers :

- Ring Imager, 4400
- Ring Scanner, 955

Configuration bar codes for these scanners are included in the *8600 Ring Scanner User’s Guide*.

The HX3 can also use the following external bar code readers:

- Wireless hand-held Bluetooth scanners are configured by scanning the engine-specific bar codes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the bar code reader.
- The body worn Bluetooth Ring Scanner module may be using a Symbol 4400 Ring Imager or a Symbol 955 Ring Scanner. The BTRS module is configured by scanning the bar codes in the *8650 Bluetooth Ring Scanner User’s Guide*.

Return to Factory Default Settings

When using any bar code reader to scan the Reset All (or equivalent) bar code with the HX3’s ring decoder, the next step is to open the Scanner applet on the HX3, click the OK button and then close it. This action will synchronize all scanner formats.

For more information see:

- Set Default Parameters for ring scanner
- Set All Defaults / Cancel Bar Codes for ring imager

These configuration bar codes are available in the:

- *8600 Ring Scanner User’s Guide* (for tethered ring scanners)
- *8650 Bluetooth Ring Scanner User’s Guide* (for Bluetooth ring scanners)

The bar codes mentioned above can be used to set or reset scan engine parameters by scanning the bar code, then saving the change. The HX3 will beep twice when a configuration bar code is successfully scanned.

Bar Code Processing Overview

Bar code processing involves several steps. Some steps may be skipped during the processing depending on user selections on the Scanner control panels. The steps are presented below in the order they are performed on the bar code data.

1. Scanned bar code is tested for a code ID and matching length (Min/Max). If it matches, it is processed per the rules in place for that symbology. If the scan does not meet the criteria for that symbology, it is processed based on the settings for All. If a code ID is not found, the bar code data is processed based on the settings for All.

1. If symbology is disabled, the scan is rejected.

2. Strip leading data bytes unconditionally.

3. Strip trailing data bytes unconditionally.

4. Parse for, and strip if found, Barcode Data strings.
5. Replace any control characters with string, as configured.
6. Add prefix string to output buffer.
7. If Code ID is not stripped, add saved code ID from above to output buffer.
8. Add processed bar code string from above to output buffer.
9. Add suffix string to output buffer.
10. Add a terminating NUL to the output buffer, in case the data is processed as a string.
11. If key output is enabled, start the process to output keys. If control characters are encountered:

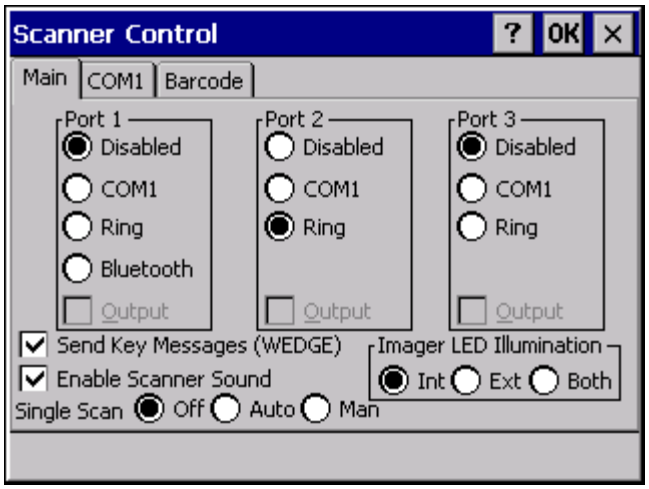
    If Translate All is set, key is translated to CTRL + char, and output.

    If Translate All is not set, and key has a valid VK code, key is output.

    Otherwise, key is ignored (not output).

The bar code data is ready to be read by applications.

Main Tab



Port

The ports are disabled until the HX3 auto-detects a device tethered to the port. Port 1 defaults to Bluetooth and Port 2 defaults to Ring when a Bluetooth enabled HX3 with ring scanner/imager is powered On.

Output

Default: Disabled. When Output is enabled, data is received from the scanner and processed via the wedge but an application can also open the WDG0: device and write data to it. An example is when a printer is connected to the same COM port as the scanner via a switch. Data can be written to the WDG device and is redirected to the associated COM port. The application must open the WDG0: port, not the COMx: port as the Wedge has exclusive rights to the COM port. If Output is not enabled, the WDG0: port can still be opened, but any attempts to write to that port will fail.

Send Key Messages (WEDGE)

Default: Enabled. When Send Key Messages (WEDGE) is checked any data scan is converted to keystrokes and sent to the active window. When this check box is not checked, the application will need to use the set of Scanner APIs to retrieve the data from the scanner driver. Note that this latter method is significantly faster than using Wedge.

Enable Internal Scanner Sound

Default: Enabled. Functionality of the internal scanner driver engine includes audible tones on good scan (at the maximum db supported by the speaker) and failed scan. Disable this parameter when good scan/bad scan sounds are to be handled by alternate means e.g., application-controlled sound files. Rejected bar codes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from an external scanner, and then the rejection of scanned bar code data by the processing causes a bad scan beep from the HX3 on the same data.

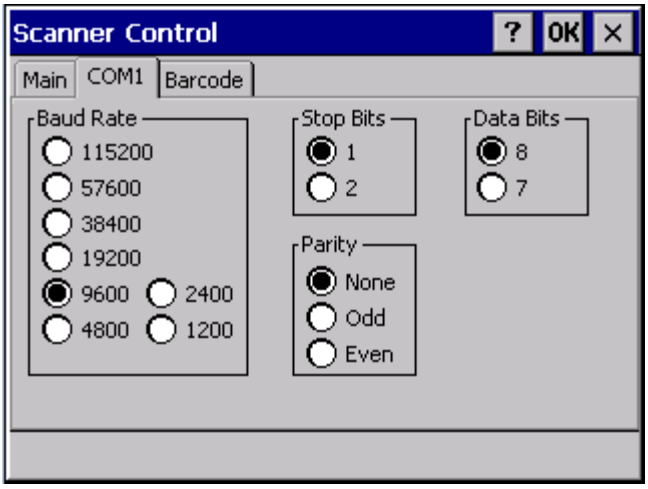
Single Scan

Single Scan determines if scanner input is inhibited after a scan until the scanner is re-enabled. Off - Single Scan mode is off. Auto - Single Scan mode is on. The scanner is disabled after a scan and automatically re-enabled by the scanner driver after retrieving the bar code data. Man - Single Scan mode is on. The scanner is disabled after a scan and the user application must call LXEScannerSSReset to re-enable the scanner. See the *CE API Programming Guide* for more details. This option is only supported on Symbol (Motorola) internal and BTRS scanners. The scanner may require a firmware upgrade to support this feature.

Imager LED Illumination

The default setting is Internal illumination. The imager has a bank of three LEDs above the imager aperture that illuminate when External or Both radio buttons are enabled. The illumination turns off when the scan is complete.

COM1 Tab



This panel sets communication parameters for any device connected to the external port.

Adjust the settings and click the OK button to save the changes. Any changes take effect immediately.

This panel does not configure the connected device. Refer to the documentation for the external connected or wireless device for information on configuring the device.

Note: COM default values are restored after a cold boot or operating system upgrade.

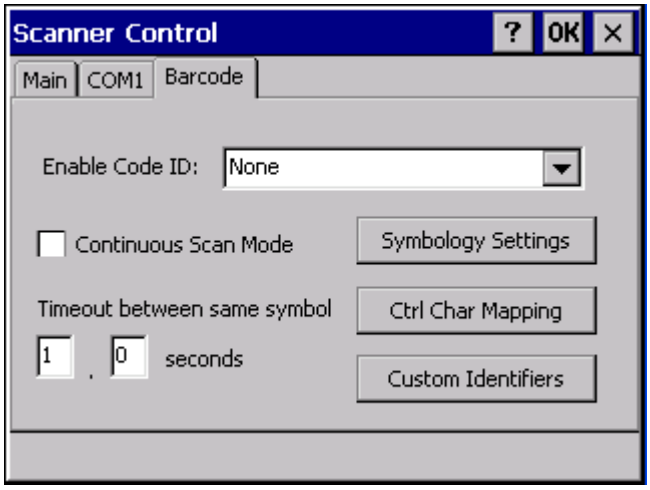
Barcode Tab

The Barcode tab contains several options to control bar code processing. Options include:

- Defining custom Code IDs
- Disable processing of specified bar code symbologies
- Rejecting bar code data that is too short or too long
- Stripping characters including Code ID, leading or trailing characters and specified bar code data strings
- Replacing control characters
- Adding a prefix and a suffix.

Notes:

- The Scanner application (Wedge) can only enable or disable bar code processing inside the Wedge software.
- The Scanner application enables or disables the Code ID that may be scanned.
- Enabling or disabling a specific bar code symbology is done manually using the configuration bar code in the *Ring Scanner User's Guide*.



Choose an option in the Enable Code ID drop-down box: None, AIM ID, Symbol ID, or Custom ID.

Symbology Settings

Individually enable or disable a bar code from being scanned, set the minimum and maximum size bar code to accept, strip Code ID, strip data from the beginning or end of a bar code, or (based on configurable Barcode Data) add a prefix or suffix to a bar code before transmission.

Ctrl Char Mapping

Define the operations the Wedge performs on control characters (values less than 0x20) embedded in bar codes.

Custom Identifiers

Defines an identifier that is at the beginning of bar code data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.

Continuous Scan Mode

Enabling Continuous Scan Mode will ensure the laser is always on and decoding. Caution: Laser beam is emitted continuously. Do not stare into the laser beam.

Note: Do not scan decoder engine configuration bar codes in this guide when Continuous scan mode is on. Configuration bar codes do not decode when scanned while the HX3 is in Continuous Mode.

Set the *Timeout between same symbol* to a value sufficient to prevent the beeper from continuously beeping when a symbol is left in the scanner's field of view.

When the bar code decoder is in continuous mode the scan button functions as an On/Off switch.

The ring decoder red LED will always be off in continuous mode. The audio beeps and green LED work the same as they do for normal trigger mode.

If scan mode, power mode, or timeout between same symbol parameters are changed using external configuration bar codes in the *later chapters of this guide t*he HX3 operating system automatically restores the parameters to their programmed settings upon a warm or cold boot and/or any change made in the control panel.

Toggling between continuous and normal trigger modes is in effect immediately upon pressing the OK button in this control panel, a warm boot is not required or necessary.

Enable Code ID

This parameter programs the scanner to transmit the specified Code ID and/or determines the type of bar code identifier being processed.

Transmission of the Code ID is enabled at the scanner for all bar code symbologies, not for an individual symbology. Code ID is sent from the scanner so the scanner driver can discriminate between symbologies.

Options

- None: Programs an internal scanner to disable transmission of a code ID. After clicking the Symbology Settings button, the only entry on the Symbology listing is All, plus any configured custom IDs. Select this option to disable Code ID processing. The bar code data is received, but is not checked for a Code ID.
- AIM: Programs an internal scanner to transmit the AIM ID with each bar code. After clicking the Symbology Settings button, the Symbology listing includes all AIM ID symbologies plus any configured custom Code IDs. Select this option to enable processing of bar codes with an AIM or custom Code ID.
- Symbol: Programs an internal scanner to transmit the Symbol ID with each bar code. After clicking the Symbology Settings button, the Symbology listing includes all Symbol ID symbologies plus any configured custom Code IDs. Select this option to enable processing of bar codes with a Symbol or custom Code ID. Note that the Symbol entry may not appear for any device equipped with an integrated imager (e.g., EV-15 imager).
- Custom: Does not change the internal scanner's Code ID transmission setting. After clicking the Symbology Settings button, the Symbology listing includes all Custom Code IDs. Select this option to enable processing of bar codes with a custom Code ID.

Notes

- When Strip: Code ID (see Symbology panel) is not enabled, the code ID is sent as part of the bar code data to an application.
- When Strip: Code ID (see Symbology panel) is enabled, the entire Code ID string is stripped (i.e., treated as a Code ID).
- UPC/EAN Codes only: The code id for supplemental bar codes is not stripped.
- When Enable Code ID is set to AIM or Symbol, Custom Code IDs appear at the end of the list of standard Code IDs.
- When Enable Code ID is set to Custom, Custom Code IDs replace the list of standard Code IDs.
- When Enable Code ID is set to Custom, AIM or Symbol Code IDs must be added to the end of the Custom Code ID. For example, if a Custom Code ID 'AAA' is created to be read in combination with an AIM ID for Code 39 ']A1', the Custom Code ID must be entered with the AIM ID code first then the Custom Code ID :]A1AAA.
- When Enable Code ID is set to None, Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog, but will be processed at the beginning of the list in the scanner driver. This allows custom IDs, based on actual code IDs, to be processed before the Code ID.
- When using the parameters in the Scanner Control Panel to manage indicators for good read/bad read decoding, the number or patterns of beeps heard may be confusing. Rejected bar codes generate a bad scan beep. In some cases, the receipt of data from an external scanner triggers a good scan beep, and then the rejection of scanned bar code data by the Scanner Control Panel processing causes a bad scan beep by the mobile device on the same data.

Bar Code – Custom Identifiers

Code IDs can be defined by the user. This allows processing parameters to be configured for bar codes that do not use the standard AIM or Symbol IDs or for bar codes that have data embedded at the beginning of the data that acts like a Code ID.

These are called custom Code IDs and are included in the Symbology drop down box in the Symbology dialog, unless Enable Code ID is set to None. When the custom Code ID is found in a bar code, the configuration specified for the custom Code ID is applied to the bar code data.

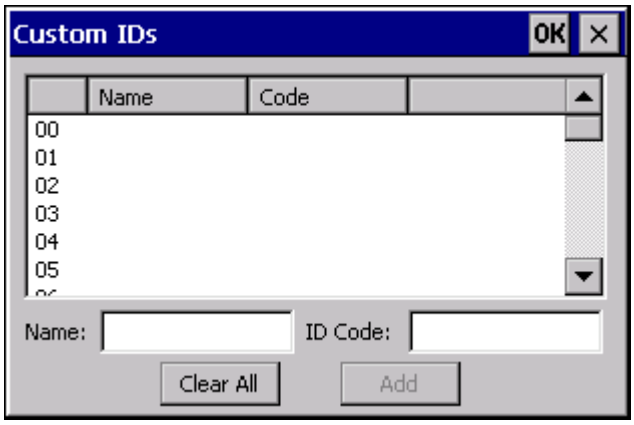
It is intended that custom code IDs are used to supplement the list of standard code IDs (if Enable Code ID is set to AIM or Symbol), or to replace the list of standard code IDs (if Enable Code ID is set to Custom).

When Enable Code ID is set to None, custom code IDs are ignored.

Note: Custom symbologies will appear at the end of the list in the Symbology dialog, and are processed at the beginning of the list in the scanner driver itself. This allows custom IDs based on actual code IDs to be processed before the code ID itself.

Note: When Strip: Code ID is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).

The dialog box shown below allows the custom Code IDs to be configured. When incoming data is checked for a custom ID code, the list is compared in the order displayed in this dialog box.



After adding, changing and removing items from the Custom IDs list, click the OK button to save changes and return to the Barcode panel.

Name text box

Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the Name and ID Code may have the same value. Name is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

ID Code text box

ID Code defines the data at the beginning of a bar code that acts as an identifier (the actual Code ID). Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

Buttons

Add

Entering data into both the Name and ID Code fields enables the Add button. Click the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Click on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and click the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double click on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is clicked, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, clicking the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button text changes to a Remove button when an item in the Custom IDs list is selected. Click the desired line item and then click the Remove button to delete it. Line items are removed one at a time. Contents of the text box fields are cleared at the same time.

Control Code Replacement Examples

Configuration Data	Translation	Example Control Character	Example Configuration	Translated Data
Ignore (drop)	The control character is discarded from the bar code data, prefix and suffix	ESCape	Ignore (drop)	0x1B in the bar code is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	STX	0x02 in a bar code is converted to the text STX.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	^M	Value 0x0d in a bar code is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass through to the application.	Horizontal Tab	\^I	Value 0x09 in a bar code is converted to the text ^I.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	0x0A	Value 0x0D in a bar code is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass through to the application.	Vertical Tab	\0x0A or 0\x0A	Value 0x0C is a bar code is converted to text 0x0A

Bar Code Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit an AIM identifier.

	Symbology				
	All	EAN-128(]C1)	EAN-13(]E0)	Intrlv 2 of 5(]IO)	Code93
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Bar Code Data		*123	1*	456	
Strip Trailing	0	0	3	3	
Prefix	aaa	bbb	ccc	ddd	
Suffix	www	xxx	yyy	zzz	

Provided that the wedge is configured with the above table, below are examples of scanned bar code data and results of these manipulations.

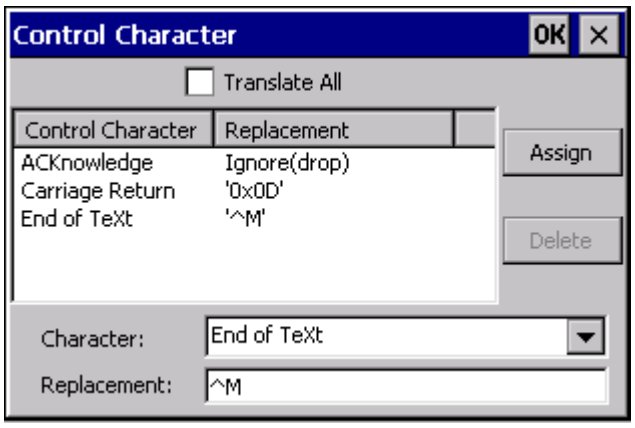
Bar Code Symbology	Raw Scanner Data	Resulting Data
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	< rejected > (too short)
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E012312345678909 87	ccc]E0234567890yyy
EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	< rejected > (too long)
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	< rejected > (disabled)
Code-93	]G0444444	< rejected > (disabled)
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	< rejected > (too short)

Note: Rejected bar codes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned bar code data by the processing causes a bad scan beep on the same data.

Bar Code - Ctrl Char Mapping

The Ctrl Char Mapping button (Control Character Mapping) activates a dialog to define the operations the Wedge performs on control characters (values less than 0x20) embedded in bar codes. Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values.

In key message mode, control characters can also be translated to their control code equivalent key sequences.



When Translate All is checked, unprintable ASCII characters (characters below 20H) in scanned bar codes are assigned to their appropriate CTRL code sequence when the bar codes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of key-strokes. If control characters are translated, the translation is performed on the bar code data, prefix, and suffix before the keystrokes are simulated.

Translate All

This option is grayed unless the user has Send Key Messages (WEDGE) on the Main tab selected.

In Key Message mode, when this option is enabled, control characters embedded in a scanned bar code are translated to their equivalent control key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad).

Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke.

Any control code without a keystroke equivalent is dropped.

Character

This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names.

When a character name is selected from the drop down box, the default text *Ignore (drop)* is shown and highlighted in the Replacement edit control. *Ignore (drop)* is highlighted so the user can type a replacement if the control character is not to be ignored.

Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplays the default *Ignore (drop)* in the Replacement edit control.

Replacement

The edit control where the user types the characters to be assigned as the replacement of the control character.

Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then clicking the Assign button. The assigned replacement is then added to the list box above the Assign button.

For example, if Carriage Return is replaced by Line Feed (by specifying ^J or 0x0A) in the configuration, the value 0x0d received in any scanned bar code (or defined in the prefix or suffix) will be replaced with the value 0x0a.

The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.

List Box

The list box shows all user-defined control characters and their assigned replacements.

All replacements are enclosed in single quotes to delimit white space that has been assigned.

Assign Button

Click this button when you want to assign the characters in the Replacement text box to the character in the Character drop down box.

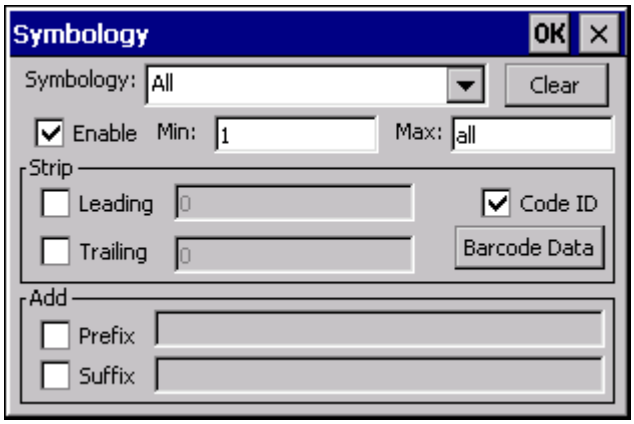
Delete Button

This button is grayed unless an entry in the list box is highlighted.

When an entry (or entries) is highlighted, and the Delete button is clicked, the highlighted material is deleted from the list box.

Bar Code - Symbology Settings

The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured. The features available on the Symbology Settings dialog include the ability to individually enable or disable a bar code from scanning, set the minimum and maximum size bar code to accept, strip Code ID, strip data from the beginning or end of a bar code, or (based on configurable Barcode Data) add a prefix or suffix to a bar code.



The Symbology drop-down box contains all symbologies supported on the HX3. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the OK button is clicked. Settings are also saved when a new Symbology is selected from the Symbology drop-down list.

Clear Button -- Clicking this button will erase any programmed overrides, returning to the default settings for the selected symbology. If Clear is pressed when All is selected as the symbology, a confirmation dialog appears, then all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

The order in which these settings are processed are:

1. Min / Max
2. Code ID
3. Leading / Trailing
4. Barcode Data
5. Prefix / Suffix

Note: When Enable Code ID is set to None on the Barcode tab and when All is selected in the Symbology field, Enable and Strip Code ID on the Symbology panel are grayed and the user is not allowed to change them, to prevent deactivating the scanner completely.

Note: When All is selected in the Symbology field and the settings are changed, the settings in this dialog become the defaults, used unless overwritten by the settings for individual symbologies. This is also true for Custom IDs, where the code IDs to be stripped are specified by the user.

*Note: In Custom mode on the Barcode tab, any Code IDs **not** specified by the user will not be stripped, because they will not be recognized as Code IDs.*

If a specific symbology's settings have been configured, a star (*) will appear next to it in the Symbology drop-down box, so the user can tell which symbologies have been modified from their defaults.

If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two.

If a symbology has not been configured (does not have an * next to it) the settings for **All** are used which is not necessarily the default.

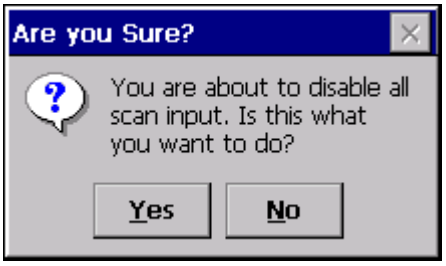
Enable

This check box enables (checked) or disables (unchecked) the symbology field.

The scanner driver searches the beginning of the bar code data for the type of ID specified in the Barcode tab -- Enable Code ID field (AIM or Symbol) plus any custom identifiers.

When a code ID match is found as the scanner driver processes incoming bar code data, if the symbology is disabled, the bar code is rejected. Otherwise, the other settings in the dialog are applied and the bar code is processed. If the symbology is disabled, all other fields on this dialog are grayed.

When there are no customized symbology settings, and the Enable check box is unchecked, while All is selected, a warning message is displayed.



Click the Yes button or the No button. Click the X button to close the dialog without making a decision.

If there are customized settings, uncheck the Enable check box for the All symbology. This results in disabling all symbologies except the customized ones.

Min

This field specifies the minimum length that the bar code data (not including Code ID) must meet to be processed.

Any bar code scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.

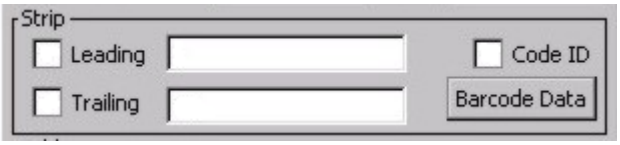
Max

This field specifies the maximum length that the bar code data (not including Code ID) can be processed. Any bar code scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999).

If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length is used instead.

Strip Leading/Trailing Control

This group of controls determines what data is removed from the bar code before the data is buffered for the application. When all values are set, Code ID takes precedence over Leading and Trailing; Barcode Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.



If the total number of characters being stripped is greater than the number of characters in the bar code data, it becomes a zero byte data string. If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

Leading

This strips the number of characters specified from the beginning of the bar code data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Trailing

This strips the number of characters specified from the end of the bar code data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Code ID

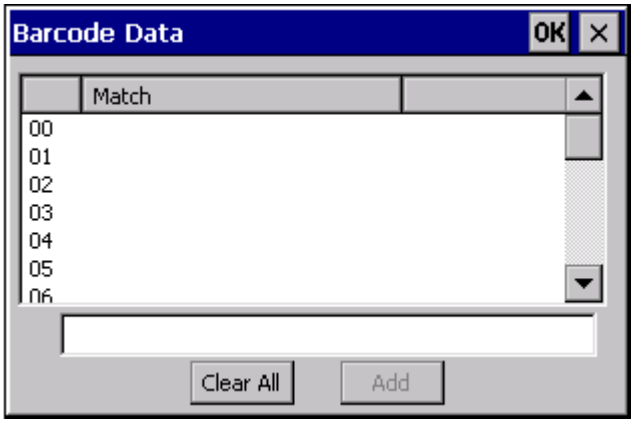
Strips the Code ID based on the type code id specified in the Enable Code ID field in the Barcode tab. By default, Code ID stripping is enabled for all symbologies (meaning code IDs will be stripped, unless specifically configured otherwise).

Bar Code Data Match List

The Barcode Data panel is used to strip data that matches the entry in the Match list from the bar code. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.

To remove an entry from the Match list, highlight the entry in the list and tap the Remove button.

Tap the OK button to store any additions, deletions or changes.



Barcode Data Match Edit Buttons

Add

Entering data into the text entry box enables the Add button. Tap the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Tap on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double tap on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is tapped, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button changes to a Remove button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

- Prefix and Suffix data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length bar code, a good beep will still be sounded, since bar code data was read from the scanner.

Match List Rules

The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains ABC and AB, in that order, incoming data with ABC will match first, and the AB will have no effect.
- When a match between the first characters of the bar code and a string from the list is found, that string is stripped from the bar code data.
- Processing the list terminates when a match is found or when the end of the list is reached.
- If the wildcard * is not specified, the string is assumed to strip from the beginning of the bar code data. The string ABC* strips off the prefix ABC. The string *XYZ will strip off the suffix XYZ. The string ABC*XYZ will strip both prefix and suffix together. More than one * in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first * is used in parsing to match the string.)
- The question mark wildcard ? may be used to match any single character in the incoming data. For example, the data AB?D will match ABCD, ABcD, or AB0D, but not ABDE.
- The Barcode Data is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of Strip: Code ID in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the bar code data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the bar code data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.

Add Prefix/Suffix Control

Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the bar code data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. See Hat Encoding (page 7-16) for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering of literal hex and hat values.

Add Prefix

To enable a prefix, check the Prefix check box and enter the desired string in the text box.

The default is disabled (unchecked) with a blank text string. When bar code data is processed, the Prefix string is sent to the output buffer before any other data.

Because all stripping operations have already occurred, stripping settings do not affect the prefix. The prefix is added to the output buffer for the Symbology selected from the pull down list.

If ‘All’ is selected, the prefix is added for any symbology that has not been specifically configured.

Add Suffix

To enable a suffix, check the Suffix check box and enter the desired string in the text box.

The default is disabled (unchecked) with a blank text string. When bar code data is processed, the Suffix string is sent to the output buffer after the bar code data.

Because all stripping operations have already occurred, stripping settings do not affect the suffix. The suffix is added to the output buffer for the Symbology selected from the pull down list.

If ‘All’ is selected, the suffix is added for any symbology that has not been specifically configured.

Note: Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g., F1), arrow keys, Page up, Page down, Home, and End.

Length Based Bar Code Stripping

Use this procedure to create symbology rules for two bar codes with the same symbology but with different discrete lengths. This procedure is not applicable for bar codes with variable lengths (falling between a maximum value and a minimum value).

Example 1:

- A normal AIM or Symbol symbology role can be created for the desired bar code ID.
- Next, a custom bar code symbology must be created using the same Code ID as the original AIM or Symbol ID rule and each rule would have unique length settings.

- *Example 2:*

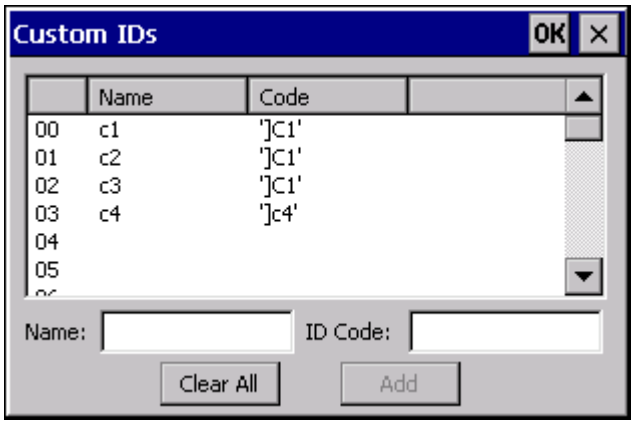
For the purposes of this example, the following sample bar code parameters will be used – EAN 128 and Code 128 bar codes. Some of the bar codes start with ‘00’ and some start with ‘01’. The bar codes are different lengths.

- 34 character length with first two characters = “01” (strip first 2 and last 18)
- 26 character length with first two characters = “01” (strip first 2 and last 10)
- 24 character length with first two characters = “01” (strip first 2 and last 8). This 24 character bar code is Code 128.
- 20 character length with first two characters = “00” (strip first 0 (no characters) and last 4)

On the Barcode tab, set Enable Code ID to AIM.

Create four custom IDs, using 1 for EAN 128 bar code and 0 for Code 128 bar code.

- c1 = Code = ‘]C1’
- c2 = Code = ‘]C1’
- c3 = Code = ‘]C0’ (24 character bar code is Code 128)
- c4 = Code = ‘]C1’

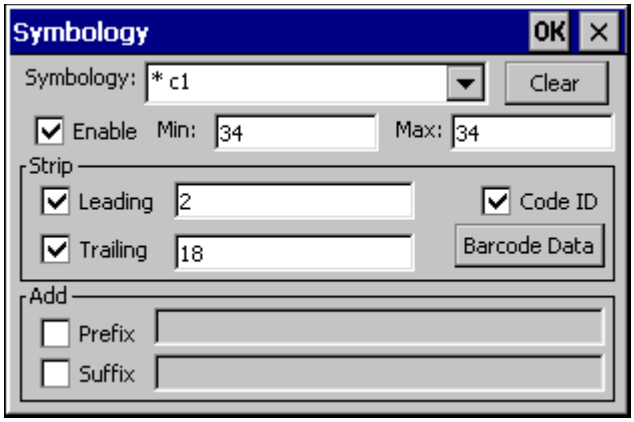


AIM custom symbology setup is assigned in the following manner:

- c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = “01”
- c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = “01”
- c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = “01”

- c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = “00”

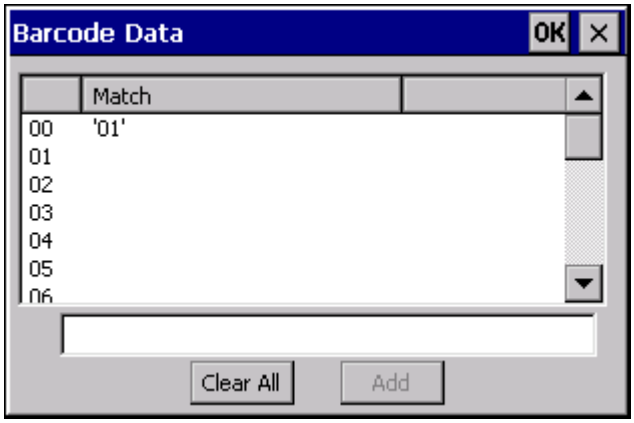
Add the AIM custom symbologies. Refer to the previous section Bar Code – Symbology Settings for instruction.



Click the Barcode Data button.

Click the Add button.

Add the data for the match codes.



Refer to the previous section Bar Code Data Match List (page 7-12) for instruction.

Scan a bar code and examine the result.

Hat Encoding

Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@
SOH	0X01	^A
STX	0X02	^B
ETX	0X03	^C
EOT	0X04	^D
ENQ	0X05	^E
ACK	0X06	^F
BEL	0X07	^G
BS	0X08	^H
HT	0X09	^I
LF	0X0A	^J
VT	0X0B	^K
FF	0X0C	^L
CR	0X0D	^M
SO	0X0E	^N
SI	0X0F	^O
DLE	0X10	^P
DC1 (XON)	0X11	^Q
DC2	0X12	^R
DC3 (XOFF)	0X13	^S
DC4	0X14	^T
NAK	0X15	^U
SYN	0X16	^V
ETB	0X17	^W
CAN	0X18	^X
EM	0X19	^Y
SUB	0X1A	^Z
ESC	0X1B	^[
FS	0X1C	^\\
GS	0X1D	^]
RS	0X1E	^^
US	0X1F	^ (Underscore)
	0X7F	^?
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~"
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~'
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z

Desired ASCII	Hex Value	Hat Encoded
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V

Desired ASCII	Hex Value	Hat Encoded
Û	DB	~[
Ü	DC	~\\
Ý	DD	~]
Þ	DE	~\^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~|
ý	FD	~}
þ	FE	~~
ÿ	FF	~^?

8 Enabler Installation and Configuration

Introduction

Although the HX3 has no display or alphanumeric keypad, HX3 control panels can be viewed and parameters manipulated using LXEConnect and ActiveSync on a connected host computer.

The HX3 does not have a touch screen. If the host computer has a touch screen, instructions using “tap” and “stylus” instead of “click” and “mouse” apply.

This section discusses supported features with Wavelink Avalanche Mobile Device Servers. This section is split into three basic areas:

- Installation
- User Interface
- Enabler Configuration

Installation

To use the Wavelink Avalanche MC System, the following items are required:

- A desktop or laptop PC on which to install the Avalanche MC Console.
- A desktop or laptop PC on which to install the Avalanche Mobile Device Server (this can be the same PC where the Avalanche MC Console is installed).
- Wavelink Avalanche MC Console 4.2 or later.
- A Wavelink Device License for each client device.

To use Avalanche Remote Control, the follow additional items are required:

- Wavelink Remote Control plug-in, 2.0 or later
- A Wavelink Remote Control License for each client device

Installing the Enabler on Mobile Devices

Supported devices have the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped. The installation files are located in the \System folder on Windows devices.

Note: Important: If the user is NOT using Wavelink Avalanche to manage their mobile device(s), the Enabler should not be installed on the mobile device(s). Doing so results in unnecessary delays when booting the device.

The Avalanche Enabler installation file HSM_ENABLER.CAB is loaded on the HX3 by Honeywell; however, the device is not configured to launch the Enabler installation file automatically. The installation application must be run manually the first time Avalanche is used.

After installation, the Enabler runs as a background application monitoring for updates. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler interface.

The RMU.CE.CAB file is placed on the device during manufacturing in the \System\RMU folder.

During the Enabler installation process, the Enabler checks for the RMU.CE.CAB file in the \System folder.

- If present, it assumes the RMU.CE.CAB file is already installed and continues.
- If the file RMU.CE.CAB file is not present, it looks for the file in the \System\RMU folder.
- If present, the Enabler copies the file to the \System folder and installs it.

At this point, the OS will automatically install the Remote Management Utility (RMU) after the HX3 reboots.

Enabler Uninstall Process

To remove the Avalanche Enabler from the HX3:

- Delete the Avalanche folder located in the \System directory.
- Warm boot the HX3.

The Avalanche folder cannot be deleted while the Enabler is running. See Stop the Enabler Service (page 8-2).

If sharing errors occur while attempting to delete the Avalanche folder, warm boot the HX3, immediately delete the Avalanche folder, and then perform another warm boot.

Note: Although the HX3 has no display or alphanumeric keypad, HX3 control panels can be viewed and parameters manipulated using LXEConnect and ActiveSync on a connected desktop/laptop computer.

Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Mobility Center Console:

1. Open the Enabler Settings Panels by tapping the Enabler icon on the HX3 desktop.
2. Select **File > Settings.**
3. Select the **Startup/Shutdown** tab.
4. Select the **Do not monitor or launch Enabler** parameter to prevent automatic monitoring upon startup.
5. Select **Stop Monitoring** for an immediate shutdown of all Enabler update functionality upon exiting the user interface.
6. Click the **OK** button to save the changes.
7. Reboot the HX3 if necessary.

Update Monitoring Overview

There are three methods by which the Enabler on the HX3 can communicate with the Mobile Device Server running on the host machine.

- Wired via a serial cable between the Mobile Device Server PC and the HX3.
- Wired via a USB connection, using ActiveSync, between the Mobile Device Server PC and the HX3.
- Wirelessly via the HX3 2.4GHz radio and an access point

After installing the Enabler on the HX3 the Enabler searches for a Mobile Device Server, first by polling all available serial ports and then over the wireless network.

The Enabler running on the HX3 will attempt to access COM1, COM2, and COM3. “Agent not found” will be reported if the Mobile Device Server is not located or a serial port is not present or available (COM port settings can be verified using the bar code wedge panels on the HX3).

The wireless connection is made using the default wireless [radio] interface on the mobile device therefore the HX3 must be actively communicating with the network for this method to succeed.

If a Mobile Device Server is found, the Enabler automatically attempts to apply all wireless and network settings from the active profile. The Enabler also automatically downloads and processes all available packages.

If the Enabler does not automatically detect the Mobile Device Server, the IP address of the Mobile Device Server can be entered on the Connect tab of the Enabler setup. See Enabler Configuration (page 8-4) for details.

Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the HX3 Enabler attempts to apply all network and wireless settings contained in the active profile.

The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler.

These local parameters cannot be overridden from the Avalanche MC Console.

The default Enabler adapter control settings are:

- Manage network settings – enabled

- Use Avalanche network profile – enabled
- Manage wireless settings – disabled

To configure the Avalanche Enabler management of the network and wireless settings:

1. Open the Enabler Settings Panels by tapping the Enabler icon on the desktop.
2. Select **File > Settings.**
3. Select the **Adapters** tab.
4. Choose settings for the **Use Manual Settings** parameter.
5. Choose settings for **Manage Network Settings**, **Manage Wireless Settings** and **Use Avalanche Network Profile**.
6. Click the **OK** button to save the changes.
7. Reboot the device.

Preparing a Device for Remote Management

Two additional utilities are necessary for remote management.

1. The Remote Management Utility (RMU) must be installed on all mobile devices first – then you can control mobile device reboot, storage RAM adjustment, real-time updates and Avalanche Enabler properties. If the RMU is not already installed on the HX3, see *Using Wavelink Avalanche to Upgrade System Baseline*. If in doubt, verify RMU.CE.CAB exists in the \System folder. If the RMU.CE.CAB file is present when the Enabler is installed, the RMU is also installed. Important: If the OS package includes double-byte Asian fonts, the storage RAM property of the RMU must be higher than the default value (40MB). If the amount of storage RAM is too low, the Enabler returns a "Mobile unit out of resources" error. To determine the minimum value required, inspect the RMU.StorageRAM>=nn parameter in the Criteria field for the OS package. Generally, this setting should be approximately 40 MB above the amount of RAM in use on the device for a standard OS and 50MB above the amount of RAM in use for an OS with Asian fonts. For example, if after installing all the software, the device shows 5MB in use, this setting should be about 45MB for a standard OS, 55 MB for an Asian font OS.
2. Use the Wireless Configuration Application (WCA) when you want to remotely manage the Summit client device. This utility is downloaded and installed in addition to the Remote Management Utility. The WCA is included when the Summit radio driver software is updated. The WCA is automatically installed when the radio driver is updated.

If the Remote Management Utility (RMU) is not present on the HX3, see *Using Wavelink Avalanche to Upgrade System Baseline.*

Using Wavelink Avalanche to Upgrade System Baseline

This procedure assumes the Avalanche Enabler is already installed on the HX3 and is already in communication with the Avalanche MC Console.

Part 1 – Bootstrapping the RMU

1. Install the RMUCEbt package into the Avalanche MC Console. Do NOT include the Reboot option as part of the configuration (i.e., the Reboot button in the "Reboot Options" branch must be unbolded).
2. Enable ONLY the RMUCEbt package in the Avalanche MC Console and update the devices. The RMU is downloaded and automatically installed.
3. Disable the RMUCEbt package in the Avalanche MC Console.
4. For each device, double-click on the device to open the Client Controls dialog box.
5. Check the Delete Orphaned Packages check box and click the Update Now button.
6. After the sync completes, uncheck Delete Orphaned Packages and close the dialog box.

Part 2 – Installing Packages

1. Enable the RMUCE package in the Avalanche MC Console.
2. Enable all remaining packages and send them down. It is important that you include the new OS package in this group (be sure to include the Enabler). If the radio is to be managed remotely, it is important to include the radio package in this group so that after the reboot the radio can automatically associate. If the radio package is not sent, the device loses connection to the network and manual configuration of the radio parameters is required.

3. Set the Reboot setting for the OS package to Auto.
4. After all packages are downloaded (this may take several minutes) the Remote Management Utility (RMU) is launched. The RMU processes all the downloaded packages. If the radio package was downloaded, the Wireless Configuration Application (WCA) is launched to process the new radio settings.
5. After the RMU finishes installing all the packages, the device is automatically coldbooted (assuming the Reboot setting was set to Auto in Step 3).
6. After the Device completes the coldboot, the RMU is autoinstalled by the OS and the previously downloaded packages are restored. Assuming at least one package has registry settings that were restored, and that package was set to reboot (either auto or prompt), the RMU then performs an automatic warmboot.
7. After the warmboot, the device is configured.
8. If the device will no longer be monitored by Wavelink Avalanche, you may remove the Enabler to eliminate boot up delays, if desired. Even if the Enabler is removed, the installed packages and their configurations continue to be restored with every reboot by the RMU.

Version Information on Mobile Devices

The VersionInfo.EXE file is included in the Remote Management Utility package downloaded to the HX3. It is stored in the \Program Files\RMU folder. When VersionInfo.EXE is opened, a dialog box is presented to the HX3 user displaying:

- Remote Management Utility (RMU) version
- Wireless Configuration Application (WCA) version

VersionInfo displays the version for each utility only after that utility has been executed at least once.

User Interface

The Enabler can be configured and controlled manually through the user interface on the HX3. This section details the functionality that can be controlled by the user or system administrator.

Screen displays shown in this section are designed to present the end-user with information graphically.

Placement of information on the screen displays may be split between one or many tabbed panels.

Standard Avalanche Enabler parameters that are not supported may be missing or dimmed (visible but unable to be edited) on the tabbed panels or screen displays.

Enabler Configuration

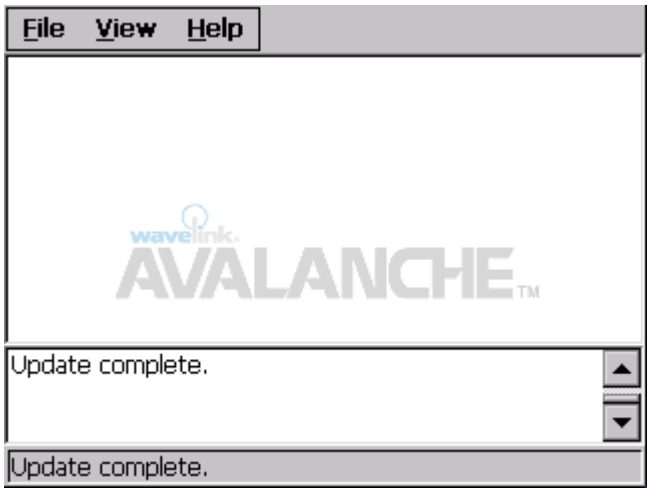
Depending on the version of the Enabler running on the HX3, the desktop Enabler icon may look like one of the following:



The available configuration options and tabs may vary by Enabler version. The examples shown in this section assume the latest version of the Enabler is installed on the HX3.

The Enabler user interface application is launched by clicking either the Enabler icon on the desktop or Taskbar or by selecting Avalanche Enabler from the Programs menu.

The opening screen presents the HX3 user with the connection status and a navigation menu.



Some parameters and features described in this section may not be available if you are not running the latest version of the Enabler. Contact Customer Support (page 14-1) for upgrades.

File Menu Options

Connect	The Connect option under the File menu allows the user to initiate a manual connection to the Mobile Device Server. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the HX3 immediately upon a successful connection.
Scan Config	The Scan Configuration feature is not supported. The Scan Config option under the File menu allows the user to configure Enabler settings using a special bar code that can be created using the Avalanche MC Console utilities. Refer to the Wavelink Avalanche Mobility Center User Guide for details.
Settings	The Settings option under the File menu allows the HX3 user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected.  The default Settings password is **system**. The password is not case-sensitive.

Avalanche Update using File > Settings

Use these menu options to setup the Avalanche Enabler on the HX3. Change the settings and save them by rebooting before connecting to the network.

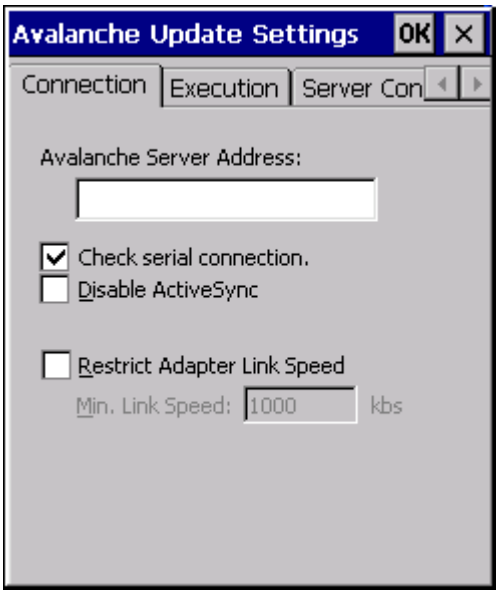
Alternatively, the Mobile Device Server can be disabled until needed (refer to the *Wavelink Avalanche Mobility Center User's Guide* for details).

Menu Options

Note: Your HX3 screen display may not be exactly as shown in the following menu options.

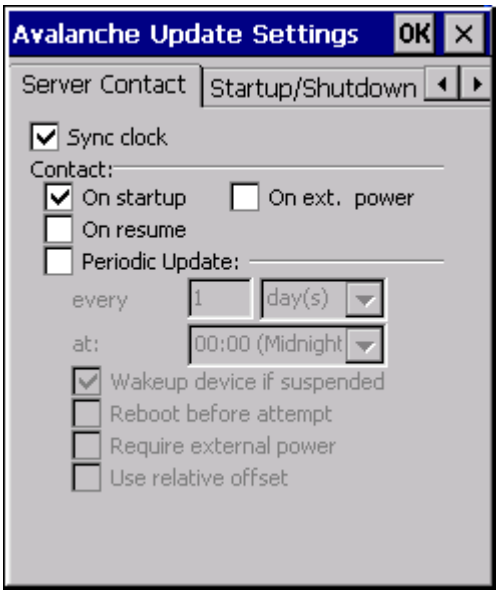
Connection (page 8-7)	Enter the IP Address or host name of the Mobile Device Server. Set the order in which serial ports or RF connections are used to check for the presence of the Mobile Device Server.
Server Contact (page 8-8)	Setup synchronization, scheduled Mobile Device Server contact, suspend and reboot settings.
Data (page 8-9)	Control when data is transferred between the HX3 and the Mobile Device Server.
Preferences (page 8-10)	Set options for Enabler startup or shutdown and logging. If the Preferences tab is not present, you may have an older version of the Enabler with the Startup/Shutdown tab.
Display (page 8-11)	Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.
Taskbar (page 8-12)	Set options for Taskbar. If the Taskbar tab is not present, you may have an older version of the Enabler with the Startup/Shutdown tab.
Execution (page 8-13)	Not available in this release.
Scan Config (page 8-14)	This option allows the user to configure Enabler settings using a special bar code that is created by the Avalanche MC Console. Scan Config not currently supported.
Shortcuts (page 8-15)	Add, delete and update shortcuts to user-allowable applications.
SaaS (page 8-16)	Configure the Enabler to connect with Avalanche on Demand.
Adapters (page 8-17)	Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.
Status (page 8-20)	View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.
Startup/Shutdown (page 8-21)	Set options for Enabler program startup or shutdown. Replaced by Preferences and Taskbar tabs in some versions of Enabler.

Connection



Avalanche Server Address	Enter the IP Address or host name of the Mobile Device Server assigned to the HX3.
Check Serial Connection	Indicates whether the Enabler should first check for serial port connection to the Mobile Device Server before checking for a wireless connection to the Mobile Device Server.
Disable ActiveSync	Disable ActiveSync connection with the Mobile Device Server.
Restrict Adapter Link Speed	Default is disabled. Minimum Link Speed dimmed. When enabled, the Enabler only allows a connection to the server if the detected link speed is greater than or equal to the specified value.

Server Contact



Note: Your HX3 screen display may not be exactly as shown above.

Note: Sync Clock

Reset the time on the HX3 based on the time on the Mobile Device Server host PC.

Contact

On Startup – Connect to the Mobile Device Server when the Enabler is accessed.

On Resume – Connect to the Mobile Device Server when resuming from Suspend mode.

On IP Change – Connect to the Mobile Device Server when the IP address of the HX3 changes.

On Ext. Power – Initiate connection to the Mobile Device Server when the device is connected to an external power source, such as based on a docking event.

Contact Periodically / Periodic Update

Allows the administrator to configure the Enabler to contact the Mobile Device Server and query for updates at a regular interval beginning at a specific time.

Wakeup device if suspended

If the time interval for periodic contact with the Mobile Device Server occurs, a mobile device that is in Suspend Mode can wakeup and process updates.

Reboot before attempt

Reboot mobile device before attempting to contact Mobile Device Server.

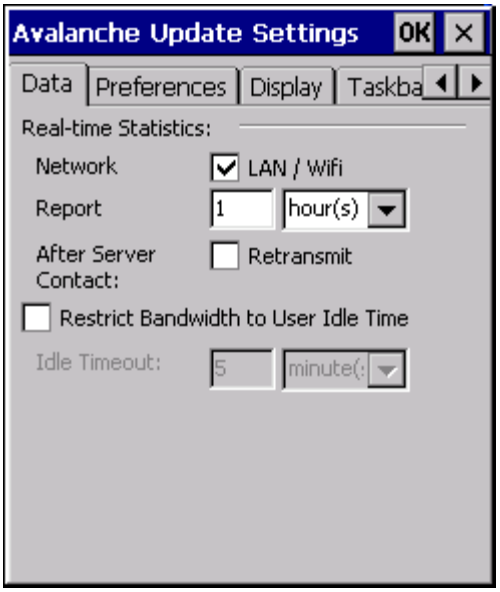
Require external power

Only connect when the mobile device has external power.

Use relative offset

Dimmed.

Data



The Data tab controls when data is transferred between the HX3 and the Mobile Device Server.

Network

When checked, the LAN/Wi-Fi network is enabled to transfer statistics.

Report

Specifies the Report Interval, how frequently the Enabler reports statistics to the Mobile Device Server.

Retransmit After Server Contact

Specifies if the device sends statistics to the Mobile Device Server immediately following a connection to the server.

Restrict Bandwidth to User Idle Time

When enabled, periodic updates from the Mobile Device Server are postponed until the HX3 has been idle for the specified period of time. The default is disabled.

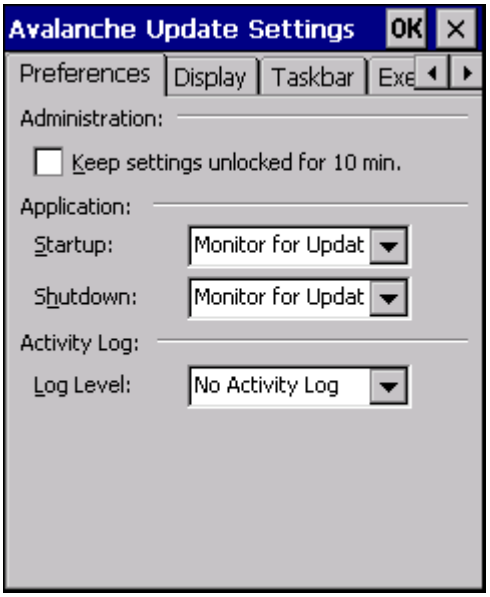
Idle timeout

Specify the length of time the device must be idle before a periodic update can run, used when the parameter above is enabled.

Preferences

For best results, use AppLock for this function. AppLock is not available for the HX3.

If the Preferences tab is not present on the Enabler installed on your device, see the equivalent options on the Startup/ Shutdown (page 8-21) tab.



Administration

By default, Keep settings unlocked for 10 minutes is disabled (check box is blank).

Application

Startup

Behavior of the Enabler when the HX3 boots up. The default is Monitor for Updates.

- Do not Monitor - When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server.
- Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
- Launch User Interface - Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.

Shutdown

Behavior of the monitor when the Enabler is exited. The default is Monitor for Updates.

- Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
- Exit Application - Terminates the monitor (requires successful password entry if a password has been configured).

Activity Log

Log Level

Use this option to control the level of detail recorded in the log file. The default is No Activity Log.

- No Activity Log - No log file is written.
- Critical - Only critical errors written to the log files.
- Error - Communication or configuration problems are written to the log file along with critical messages.
- Warning - Possible operation problems are written to the log file along with critical and error messages.
- Info - Operational information is written to the log file.

- Debug - The most detailed log file.

Display Level

Use this option to control the level of detail shown on the main Enabler screen. The default is Basic Output.

- Basic Output - General information is displayed.
- Critical - Critical errors are displayed in addition to those above.
- Error - Communication or configuration problems are displayed in addition to those above.
- Warning - Possible operation problems are displayed in addition to those above.
- Info - Operational information is displayed in addition to those above.
- Debug - The most detailed list is displayed.

Display

The user interface for the Enabler can be configured to dynamically change based on the status of the HX3 connection with the Mobile Device Server.

At startup

Default is Half Screen. Options are Half screen, Hidden or Full screen.

On connect

Default is As Is. Options are As is, Half screen, or Full screen.

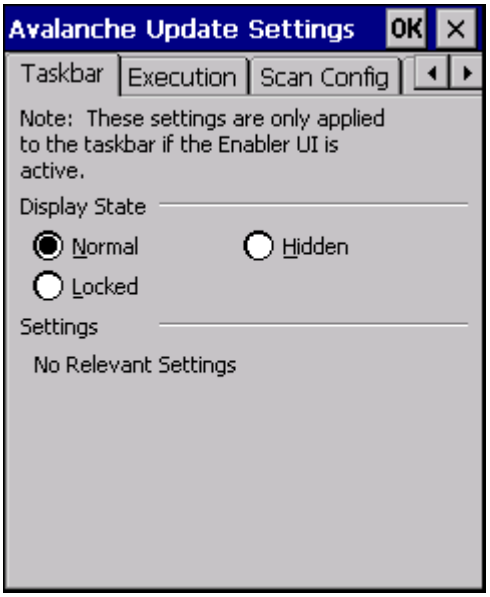
Normal

Default is As Is. Options are Half screen, Hidden or As Is.

Taskbar

For best results, use AppLock for this function. AppLock is not available for the HX3.

If the Taskbar tab is not present on the Enabler installed on your device, see the equivalent options on the Startup/ Shutdown (page 8-21) tab.

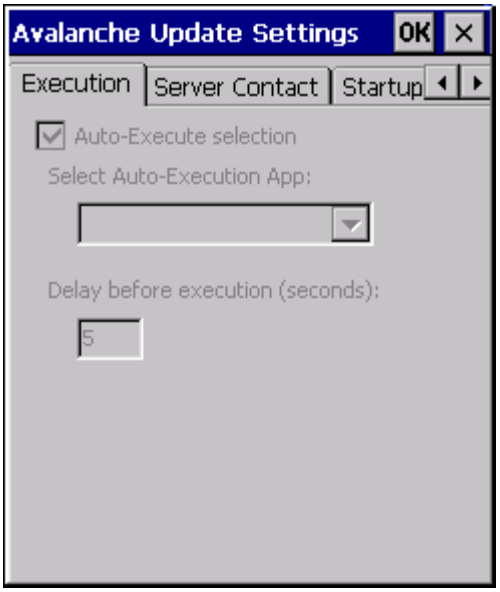


The Display State options control the appearance of the taskbar while using the Enabler interface.

- Normal - taskbar is visible, taskbar icons function normally.
- Hidden - taskbar is not displayed
- Locked - taskbar is visible, but most icons are hidden or for information only.

Execution

Note the dimmed options on this HX3 panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.



Auto-Execute Selection

An application that has been installed with the Avalanche Management system can be run automatically following each boot.

Select Auto-Execute App

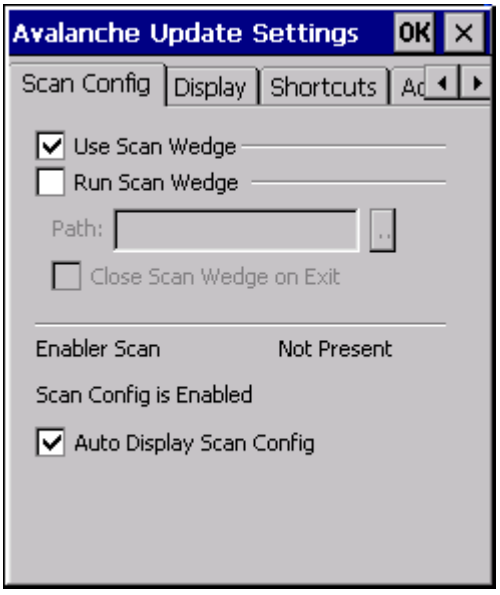
The drop-down box provides a list of applications that have been installed with the Avalanche Management System.

Delay before execution

Time delay before launching Auto-Execute application.

Scan Config

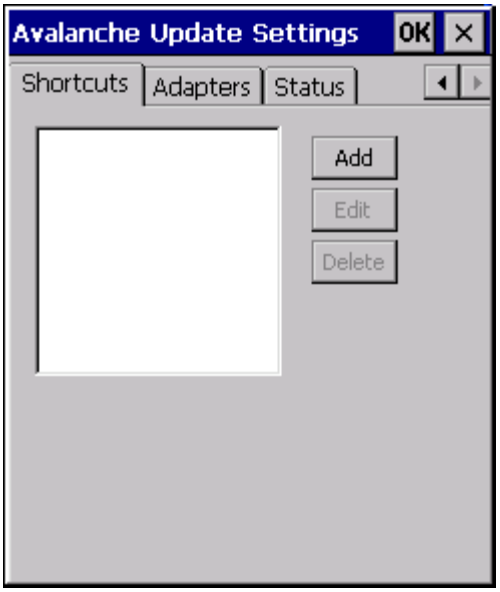
For best results, use eXpress Config and eXpress Scan for this function. eXpress Scan is included with the updated HX3 enablers.



Scan Config functionality is a standard option of the Wavelink Avalanche MC system but is not currently supported on the HX3.

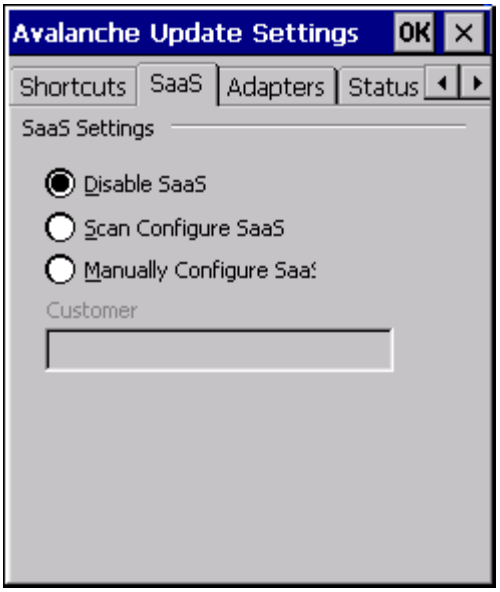
Shortcuts

For best results, use AppLock for this function. AppLock is not available for the HX3.



Configure shortcuts to other applications on the HX3. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

SaaS



Use to configure the Enabler to connect with Avalanche on Demand. This is a Software-as-a-Service version of Avalanche. Using either of the SaaS configuration options below assumes the user has registered with Wavelink.

Disable SaaS

No SaaS connection is used.

Scan Configure SaaS

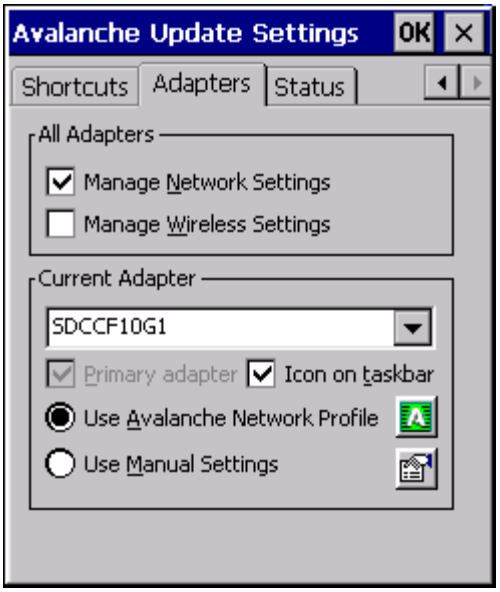
Scan bar codes printed from within the Avalanche Console to configure the Enabler for the SaaS connection.

Manually Configure SaaS

Manually enter the SaaS connection information. Enter the server address on the Connection tab and the customer ID in the Company text box.

Adapters

Note: Review the network settings configuration utilities and the default values before setting All Adapters to Enable in the Adapters applet.



Manage Network Settings

When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.

Manage Wireless Settings

When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is disabled by default. For Summit clients, Manage Wireless Settings should not be checked as configuration packages provide more radio configuration options.

Current Adapter

Lists all network adapters currently installed on the HX3.

Primary Adapter

Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).

Icon on taskbar

Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.

Use Avalanche Network Profile

The Enabler will apply all network settings sent to it by the Mobile Device Server.

Avalanche Icon(varies by Enabler version)

Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.

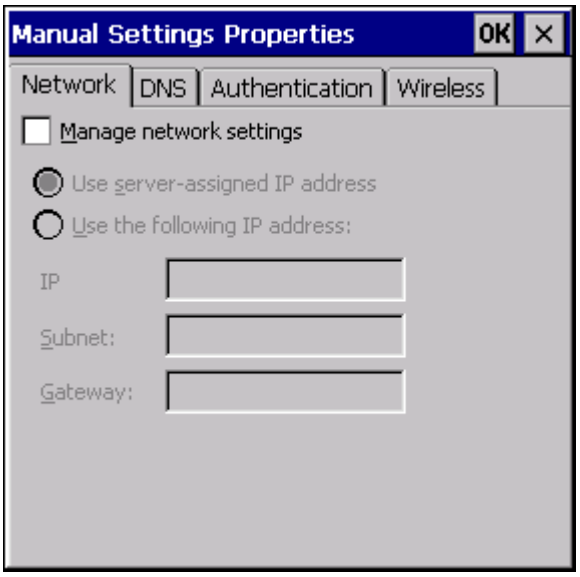
Use Manual Settings

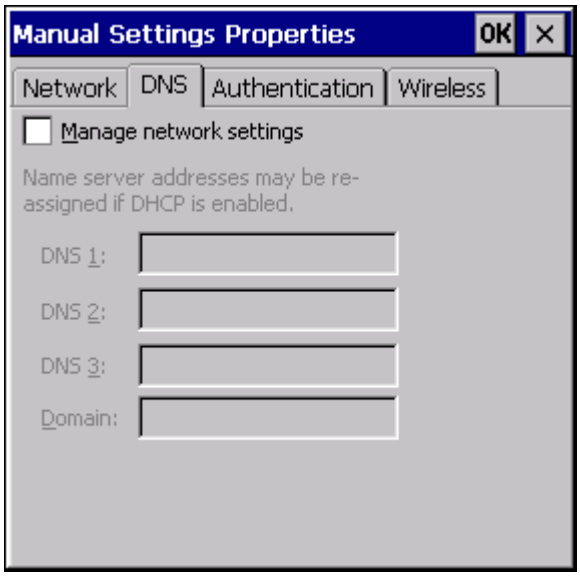
When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche MC Console and use only the network settings on the HX3.

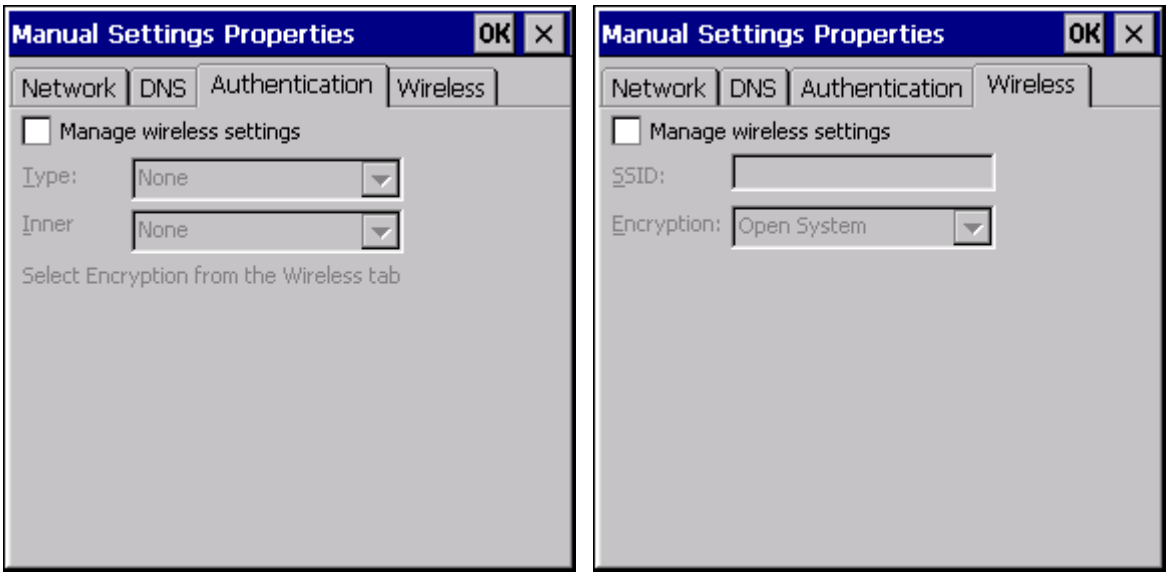
Properties Icon

Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:

Note: A reboot may be required after enabling or disabling these options.







The Authentication tab may not be present in all versions of the Enabler.

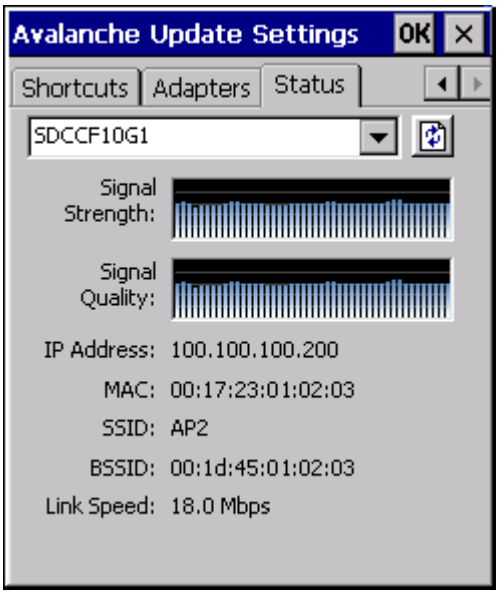
It is not recommend to enable “Manage Wireless Settings” for Summit Client devices.

When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global Manage wireless settings and Manage network settings options are enabled on the Adapters panel. Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

Status

The Status panel displays the current status of the HX3 network adapter selected in the drop down box. Note the availability of the Windows standard Refresh button.

When the Windows Refresh button is tapped, the signal strength, signal quality and link speed are refreshed for the currently selected adapter. It also searches for new adapters and may cause a slight delay to refresh the contents of the drop-down menu.

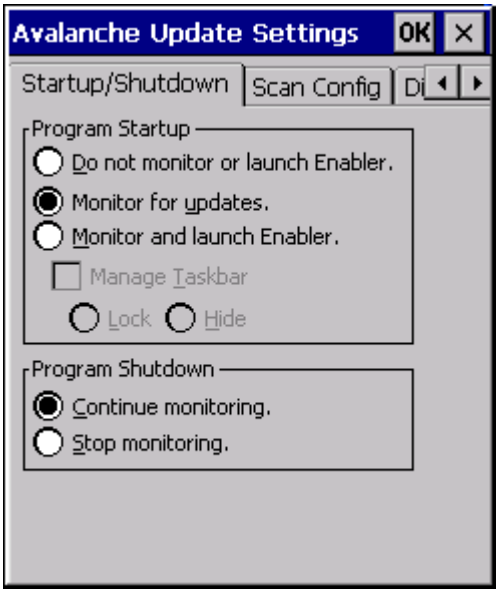


Link speed indicates the speed at which the signal is being sent from the adapter to the HX3. Speed is dependent on signal strength.

Startup/Shutdown

For best results, use AppLock to manage the taskbar. AppLock is not available on the HX3.

If the Startup/Shutdown tab is not present on the Enabler installed on your device, see the equivalent options on the Preferences (page 8-10) tab and the Taskbar (page 8-12) tab.



Do not monitor or launch Enabler

When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server.

Monitor for updates

Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.

Monitor and launch Enabler

Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.

Manage Taskbar (Lock or Hide)

Note the dimmed options. The Enabler can restrict user access to other applications when the user interface is accessed by either locking or hiding the taskbar.

Program Shutdown (Continue or Stop monitoring)

The system administrator can control whether the Enabler continues to monitor the Mobile Device Server for updates once the Enabler application is exited.

Exit

The Exit option is password protected. The default password is **leave**. The password is not case-sensitive.

Depending on the behavior chosen for the Shutdown parameter, the following screen may be displayed:

Note: The icon on the screen above may differ based on the version of the Enabler installed on the HX3.

Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche applet.

Using Remote Management

1. Configure the radio to connect to the network running the Mobile Device Server. After the HX3 is connected, proceed to step 2.
2. If it is desired to configure the radio using the Summit package, add the configured package to the Wavelink Avalanche MC Console and enable it.
3. Verify RMU.CE.CAB exists in the \System\RMU folder.
4. Double click the HX3 enabler CAB file in the \System folder.
5. The enabler automatically launches after installation and contacts the Mobile Device Server. The Avalanche MC Console connected to that Mobile Device Server identifies the remote device and performs a sync. This downloads any available packages available for the HX3.

Using eXpress Scan

If the HX3 has an eXpress Scan icon on the desktop, eXpress Scan may be used for the initial configuration of the device.

If the eXpress Scan icon is not present on the desktop, install the Enabler. If the icon is still not present, the Enabler must be updated.

If the eXpress Scan icon is present, follow these steps to configure the HX3 to connect with the wireless network and the Mobile Device Server.

Step 1: Create Bar Codes

Bar codes are created with the eXpress Config utility on the desktop/laptop computer, not the mobile device. Depending on the bar code length and the number of parameters selected, eXpress Config generates one or more bar codes for device configuration. The bar codes contain configuration parameters for the wireless client in the mobile device and may also specify the address of the Mobile Device Server.

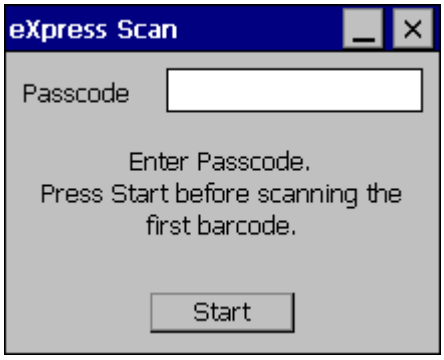
Bar codes should be printed at a minimum of 600 dpi.

See *Using Wavelink Avalanche* for details on creating bar codes.

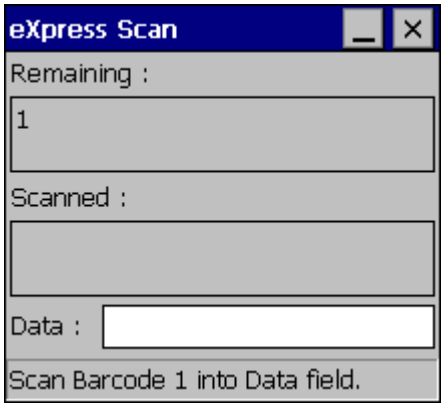
Step 2: Scan Bar Codes

For each mobile device to be configured, follow these instructions.

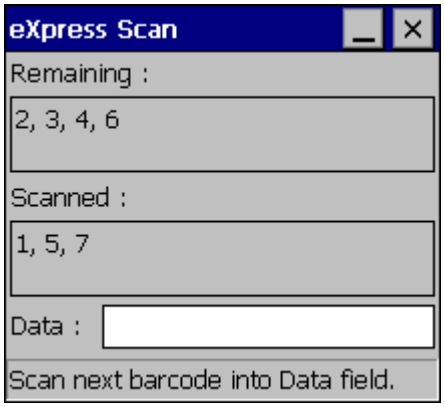
1. Start eXpress Scan on the HX3 by double clicking the eXpress Scan icon.
2. Enter the bar code password, if any.



3. Click Start.
4. Bar code 1 must be scanned first. The scanned data is displayed in the “Data” text box. The password, if any, entered above is compared to the password entered when the bar codes were created.



5. If the passwords match, the bar code data is processed and the screen is updated to reflect the number of bar codes included in the set.
6. If the passwords do not match, an error message is displayed. The current screen can be closed using the X box in the upper right corner. The password can be re-entered and Bar Code 1 scanned again.



7. The remaining bar codes may be scanned in any order. After a bar code is scanned, that bar code is removed from the "Remaining:" list and placed in the "Scanned:" list.

Step 3: Process Completion

After the last bar code is scanned, the settings are automatically applied.

Once configured, the HX3 is warmbooted. Once connected to the wireless network and the Mobile Device Server, any software updates and additional configuration data are downloaded.

9 Wireless Network Configuration

Introduction

Although the HX3 has no display or alphanumeric keypad, HX3 control panels can be viewed and parameters manipulated using LXEConnect and ActiveSync on a connected host computer.

Note: The HX3 does not have a touch screen. If the host computer has a touch screen, instructions using "tap" and "stylus" instead of "click" and "mouse" apply.

Note: The Summit client device is either an 802.11g radio, capable of both 802.11b and 802.11g data rates or an 802.11a radio, capable of 802.11a, 802.11b and 802.11g data rates. The radio can be configured for no encryption, WEP encryption or WPA security.

Security options supported are:

- No Security (page 9-19)
- WEP (page 9-20)
- LEAP (page 9-21)
- WPA PSK (page 9-31)
- WPA/LEAP (page 9-26)
- PEAP/MSCHAP (page 9-22)
- PEAP/GTC (page 9-24)
- EAP-TLS (page 9-29)
- EAP-FAST (page 9-27)

Important Notes

⚠	It is important that all dates are correct on the HX3 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.
⚠	It may be necessary to upgrade radio software in order to use certain Summit Client Utility (SCU) features. Contact Customer Support (page 14-1) for details.
⚠	When using the 802.11a radio, the U-NII 1 band is the preferred band for indoor operation. For regulatory domains in which the U-NII 3 band is allowed, the following channels are supported: 149, 157 and 161. The AP must be configured accordingly.

After making any changes to the wireless configuration, warmboot the HX3.

Summit Client Utility

Note: When making changes to profile or global parameters, the device should be warmbooted afterwards.

Select the Summit Client Utility using the Start button or tap the Summit Tray Icon (if present).

The Main Tab (page 9-3) provides information, admin login and active profile selection.

Profile specific parameters are found on the Profile Tab (page 9-5) The parameters on this tab can be set to unique values for each profile. This tab was labeled Config in early versions of the SCU.

The Status Tab (page 9-9) contains information on the current connection.

The Diags Tab (page 9-10) provides utilities to troubleshoot the radio.

Global parameters are found on the Global Tab (page 9-11). The values for these parameters apply to all profiles. This tab was labeled Global Settings in early versions of the SCU.

Help

Help is available by clicking the ? icon in the title bar on most SCU screens. The SCU help may also be accessed by selecting **Start > Help** and tapping the Summit Client Utility link. The SCU does not have to be accessed to view the help information using this option.

Summit Tray Icon

 The Summit tray icon provides access to the SCU and is a visual indicator of radio status

The Summit tray icon is displayed when:

- The Summit radio is installed and active
- The Windows Zero Config utility is not active
- The Tray Icon setting is On

Click the icon to launch the SCU. Use the tray icon to view the radio status:

	The radio is not currently associated or authenticated to an Access Point
	The signal strength for the currently associated/authenticated Access Point is less than -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -71 dBm to -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -51 dBm to -70 dBm
	The signal strength for the currently associated/authenticated Access Point is greater than -50 dBm

Wireless Zero Config Utility and the Summit Radio

The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating that Wireless Zero Config application is enabled but the connection is inactive at this time (the device is not connected to a network). The WZC icon may not be visible until control is passed to the WZC utility as described below.

You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network. As the Wireless Zero Configuration Utility cannot control the complete set of security features of the radio, it is recommended to use the Summit Client Utility to connect to your network.

Using the Wireless Zero Config Utility

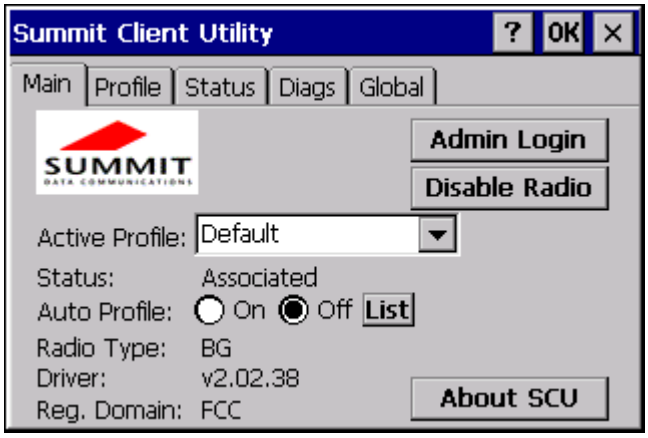
1. Select ThirdPartyConfig in the Active Profile drop down list as the active profile.
2. Warmboot the device. The Summit Client Utility passes control to Wireless Zero Config and the WZC Wireless Information control panel. Using the options in the Wireless Zero Config panels, setup radio and security settings. There may be a slight delay before the Wireless Zero Config icon indicates the status of the connection.

Switching Control to SCU

1. To switch back to SCU control, select any other profile in the SCU Active Config drop down list, except ThirdPartyConfig.
2. Warmboot the device. Radio control is passed to the SCU.

Main Tab

Setting	Default
Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	FCC or ETSI



The Main tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version
- Driver version
- Radio Type (BG is an 802.11 b/g radio, ABG is an 802.11 a/b/g radio).
- Regulatory Domain
- Copyright Information can be accessed by tapping the About SCU button
- Active Config profile / Active Profile name
- Status of the client (Down, Associated, Authenticated, etc.).

The Active Profile can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. Perform a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Admin login password has been entered and accepted.

When the profile named “ThirdPartyConfig” is chosen as the active profile, the Summit Client Utility passes control to Windows Zero Config for configuration of all client and security settings for the network module.

The Disable Radio button can be used to disable the network card. Once disabled, the button label changes to Enable Radio. By default the radio is enabled.

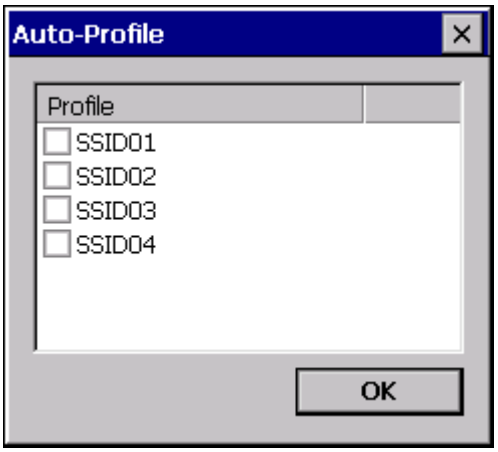
The Admin Login button provides access to editing wireless parameters. Profile and Global may only be edited after entering the Admin Login password.

The password is case-sensitive.

Once logged in, the button label changes to Admin Logout. To logout, either tap the Admin Logout button or exit the SCU without tapping the Admin Logout button.

Auto Profile

Auto Profile allows the user to configure a list of profiles that the SCU can search when a radio connection is lost. After using the Profile tab to create any desired profiles, return to the Main tab. To specify which profiles are to be included in Auto Profile, click the List button.



The Auto Profile selection screen displays all currently configured profiles. Click on the check box for any profiles that are to be included in Auto Profile selection then click ok to save.

To enable Auto Profile, click the On button on the Main tab.

When Auto Profile is On, if the radio goes out of range from the currently selected profile, the radio then begins to attempt to connect to the profiles listed under Auto Profile.

The search continues until:

- the SCU connects to and, if necessary, authenticates with, one of the specified profiles or
- the Off button is clicked to turn off Auto Profile.

Note: Do not include any profiles with an Ad Hoc Radio Mode in this listing.

Admin Login

To login to Administrator mode, tap the Admin Login button.

Once logged in, the button label changes to Admin Logout. The admin is automatically logged out when the SCU is exited. The Admin can either tap the Admin Logout button, or the OK button to logout. The Administrator remains logged in when the SCU is not closed and a Suspend/Resume function is performed.

Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap OK. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the Global tab.

The end-user can:

- Turn the radio on or off on the Main tab.
- Select an active Profile on the Main tab.
- View the current parameter settings for the profiles on the Profile Tab (page 9-5).
- View the global parameter settings on the Global Tab (page 9-11).
- View the current connection details on the Status Tab (page 9-9).
- View radio status, software versions and regulatory domain on the Main Tab (page 9-3).
- Access additional troubleshooting features on the Diags Tab (page 9-10).

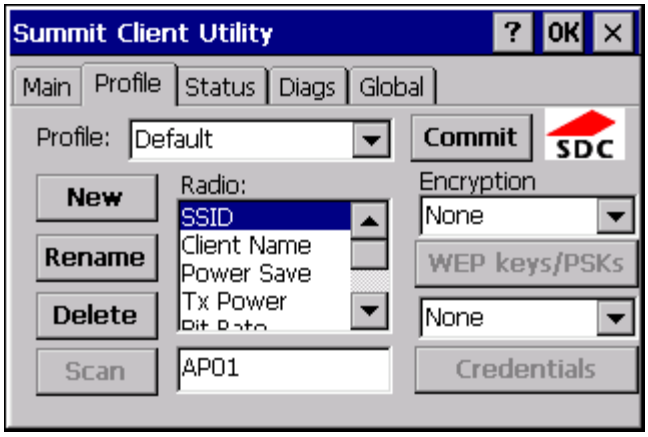
After Admin Login, the end-user can also:

- Create, edit, rename and delete profiles on the Profile Tab (page 9-5).
- Edit global parameters on the Global Tab (page 9-11).
- Enable/disable the Summit tray icon in the taskbar.

Profile Tab

Note: Tap the Commit button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the Commit button, changes are not saved!

Setting	Default
Profile	Default
SSID	Blank
Client Name	Blank
Power Save	Fast
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	See Profile Parameters (page 9-7) for default
Auth Type	Open
EAP Type	None
Encryption	None



When logged in as an Admin, use the Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in as Admin. The Profile tab was previously labeled Config.

Buttons

Commit

Saves the profile settings made on this screen. Settings are saved in the profile.

Credentials

Allows entry of a username and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.

Delete

Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.

New

Creates a new profile with the default settings (see Profile Parameters) and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.

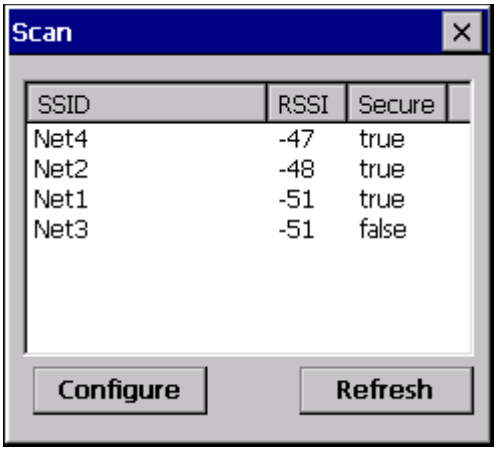
Rename

Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.

Scan

Opens a window that lists access points that are broadcasting their SSIDs. Tap the Refresh button to view an updated list of APs. Each AP's SSID, its received signal strength indication (RSSI) and whether or not data encryption is in use (true or false). Sort the list by tapping on the column headers.

If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security.



If you are logged in as an Admin, tap an SSID in the list and tap the Configure button, you return to the Profile window to recreate a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as "_1" if a profile with the SSID as its name exists already).

WEP Keys / PSK Keys

Allows entry of WEP keys or pass phrase as required by the type of encryption.

Note: Unsaved Changes – The SCU will display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from this tab.

Profile Parameters

Parameter	Default	Description
Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g., Access Points.
Power Save	Fast	Power save mode. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode). When using power management, use FAST for best throughput results.
Tx Power	Maximum	Maximum setting regulates Tx power according to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW, or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device. Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, PEAP-TLS, EAP-TTLS, or EAP-TLS. EAP Type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.
Encryption	None	Type of encryption to be used to protect transmitted data. Available options may vary by SCU version. Options are: None, WEP (or Manual WEP), WEP EAP (or Auto WEP), WPA PSK, WPA TKIP, WPA CCKM, WPA2 PSK, WPA2 AES, or WPA2 CCKM. CKIP is not supported in the HX3. The Encryption type chosen determines if the WEP Keys / PSK Keys button is active and also determines the available entries in the WEP or PSK pop-up window.

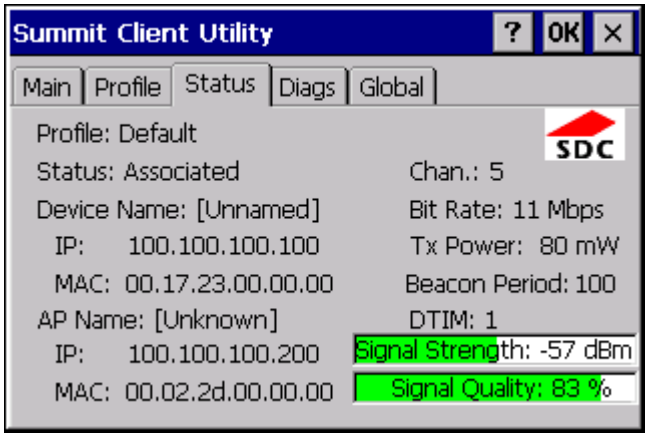
Parameter	Default	Description
Radio Mode	BG Radio: BG Rates Full or A Radio: BGA Rates Full	Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio (802.11b/g or 802.11a/b/g) installed in the mobile device. Options: B rates only (1, 2, 5.5 and 11 Mbps) BG Rates Full (All B and G rates) G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) BG optimized or BG subset (1, 2, 5.5, 6, 11, 24, 36 and 54 Mbps) A rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps) ABG Rates Full (All A rates and all B and G rates with A rates preferred) BGA Rates Full (All B and G rates and all A rates with B and G rates preferred) Ad Hoc (when connecting to another client device instead of an AP) Default: BG Rates Full (for 802.11b/g radios) BGA Rates Full (for 802.11a/b/g radio) BG radio only – Previous SCU versions may have the default set as BG Rates Full. Depending on the SCU version, either BG Optimized or BG subset is the default.It is important the Radio Mode parameter correspond to the AP to which the device is to connect. For example, if this parameter is set to G rates only, the HX3 may only connect to APs set for G rates and not those set for B and G rates.

The options for the Radio Mode parameter should be set, based on the antenna configuration, as follows:

Antenna Configuration	Radio Mode
A Main and A Aux	ABG Rates Full BGA Rates Full
A Main and A Aux	A Rates Only
BG Main and BG Aux	B Rates Only G Rates Only BG Rates Full BG Subset

Contact Customer Support (page 14-1) if you have questions about the antenna(s) installed in your HX3.

Status Tab



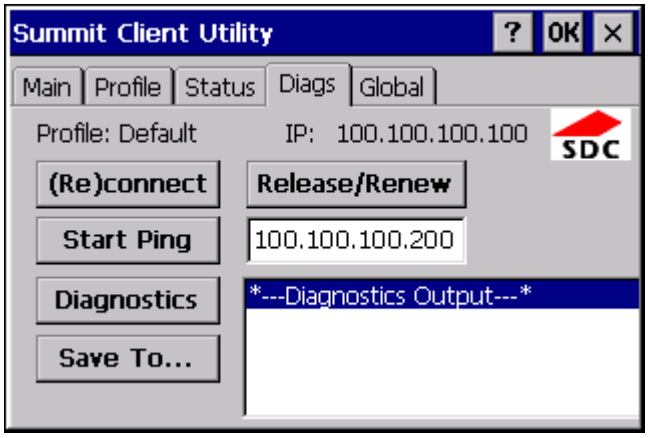
This screen provides information on the radio:

- The profile being used.
- The status of the radio card (down, associated, authenticated, etc.).
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- Channel currently being used for wireless traffic.
- Bit rate in Mbit.
- Current transmit power in mW.
- Beacon period – the time between AP beacons in kilomicroseconds (one kilomicrosecond = 1,024 microseconds).
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Signal strength (RSSI) displayed in dBm and graphically.
- Signal quality, a measure of the clarity of the signal displayed in percentage and graphically.

There are no user entries on this screen.

Note: After completing radio configuration, it is a good idea to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags Tab



The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

(Re)connect

Use this button to apply (or reapply) the current profile and attempt to associate or authenticate to the wireless LAN. All activity is logged in the Diagnostic Output box on the lower part of the screen.

Release/Renew

Obtain a new IP address through release and renew. All activity is logged in the Diagnostic Output box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed above this button.

Start Ping

Start a continuous ping to the IP address specified in the text box to the right of this button. Once the button is clicked, the ping begins and the button label changes to Stop Ping. Clicking the button ends the ping. The ping also ends when any other button on this screen is clicked or the user browses away from the Diags tab. The results of the ping are displayed in the Diagnostic Output box.

Diagnostics

Also attempts to (re)connect to the wireless LAN. However, this option provides more data in the Diagnostic Output box than the (Re)connect option. This data dump includes radio state, profile settings, global settings, and a list of broadcast SSID APs.

Save To…

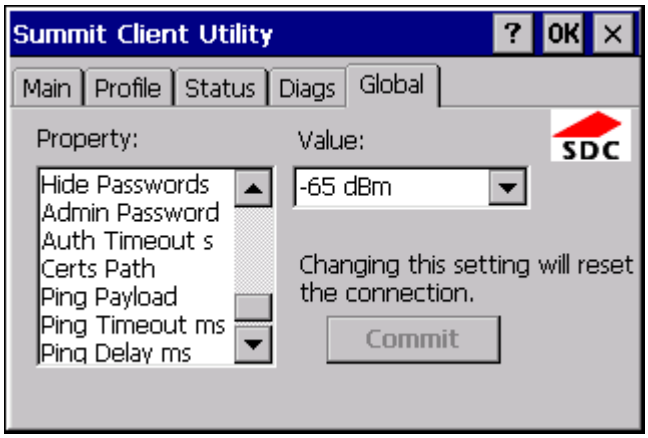
Use this to save the results of the diagnostics to a text file. Use the explorer window to specify the name and location for the diagnostic file. The text file can viewed using an application such as WordPad.

Global Tab

The parameters on this panel can only be changed when an Admin is logged in with a password. The current values for the parameters can be viewed by the general user without requiring a password.

Note: Tap the Commit button to save changes. If the panel is exited before tapping the Commit button, changes are not saved!

Setting	**Default**
Roam Trigger	-65 dBm
Roam Delta	5 dBm
Roam Period	BG: 10 sec. A: 5 sec.
BG Channel Set	Full
DFS Channels	Off
Ad Hoc Channel	1
Aggressive Scan	On
CCX Features	BG: Off A: Optimized
WMM	Off
Auth Server	Type 1
TTLS Inner Method	Auto-EAP
PMK Caching	Standard
WAPI	Off (dimmed)
TX Diversity	BG: On A: Main Only
RX Diversity	BG: On-Start on Main A: Main Only
Frag Threshold	2346
RTS Threshold	2347
LED	Off
Tray Icon	On
Hide Password	On
Admin Password	SUMMIT (or blank)
Auth Timeout	8 seconds
Certs Path	System
Ping Payload	32 bytes
Ping Timeout	5000 ms
Ping Delay ms	1000 ms



Custom Parameter Option

Honeywell does not support the parameter Custom option. The parameter value is displayed as “Custom” when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter’s drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the “custom” value in the registry.

Global Parameters

Parameter	Default	Description
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom. Available options may vary by SCU revision.
Roam Delta	5 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom. Roam delta dBm may vary by SCU revision.
Roam Period	BG: 10 sec. A: 5 sec.	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.
BG Channel Set	Full	Defines the 2.4GHz channels to be scanned for an AP when the radio is contemplating roaming. By specifying the channels to search, roaming time may be reduced over scanning all channels. Options are: Full (all channels) 1,6,11 (the most commonly used channels) 1,7,13 (for ETSI and TELEC radios only) Custom.
DFS Channels	Off	Support for 5GHZ 802.11a channels where support for DFS is required. Options are: On, Off, Optimized. Not supported (always off) in some releases.

Parameter	Default	Description
Ad Hoc Channel	1	Use this parameter when the Radio Mode profile parameter is set to Ad Hoc. Specifies the channel to be used for an Ad Hoc connection to another client device. If a channel is selected that is not supported by the by the radio, the default value is used. Options are: 1 through 14 (the 2.4GHz channels) 36, 40, 44, 48 (the UNII-1 channels)
Aggressive Scan	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel. Options are: On, Off
CCX or CCX Features	BG: Off A: Optimized	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. Options are: Full - Use Cisco IE and CCX version number, support all CCX features. The option known as “On” in previous versions. Optimized –Use Cisco IE and CCX version number, support all CCX features except AP assisted roaming, AP specified maximum transmit power and radio management. Off - Do not use Cisco IE and CCX version number. Cisco IE = Cisco Information Element.
WMM	Off	Use of Wi-Fi Multimedia extensions. Options are: On, OffDevices running Windows XP can change the default value. Devices running all other OS cannot change the default value.
Auth Server	Type 1	Specifies the type of authentication server. Options are: Type 1 (ACS server) and Type 2 (non-ACS server)
TTLS Inner Method	Auto-EAP	Authentication method used within the secure tunnel created by EAP-TTLS. Options are: AUTO-EAP (Any available EAP method) MSCHAPV2 MSCHAP PAP CHAP EAP-MSCHAPV2
PMK Caching	Standard	Type of Pairwise Master Key (PMK) caching to use when WPA2 is in use. PMK caching is designed to speed up roaming between APs by allowing the client and the AP to cache the results of 802.1X authentications, eliminating the need to communicate with the ACS server. Standard PMK is used when there are no controllers. The re-authentication information is cached on the original AP. The client and the AP use the cached information to perform the four-way handshake to exchange keys. Opportunistic PMK (OPMK) is used when there are controllers. The re-authentication information cached on the controllers. The client and the controller behind the AP use the cached information to perform the four-way handshake to exchange keys. If the selected PMK caching method is not supported by the network infrastructure, every roam requires full 802.11X authentication, including interaction with the ACS server. If the active profile is using WPA2 CCKM, the global PMK Caching setting is ignored and the client attempts to use CCKM. Options are: Standard, OPMK This change does not take effect until after a Suspend/Resume cycle.

Parameter	Default	Description
WAPI	Off	Default is Off and dimmed (cannot be changed).
TX Diversity	BG: On A: Main Only	How to handle antenna diversity when transmitting packets to the Access Point. Options are: Main only (use the main antenna only) Aux only (use the auxiliary antenna only) On (use diversity or both antennas). The options for the TX Diversity parameter should be set, based on the antenna configuration, as follows: Antenna Configuration: A Main and BG Main. TX Diversity: Main only. Antenna Configuration: A Main and A Aux. TX Diversity On. Antenna Configuration: BG Main and BG Aux. TX Diversity: On. Contact Customer Support (page 14-1) if you have questions about the antenna(s) installed in your HX3.
RX Diversity	BG: On-Start on Main A: Main Only	How to handle antenna diversity when receiving packets from the Access Point. Options are: Main Only (use the main antenna only) Aux Only (use the auxiliary antenna only) On-start on Main (on startup, use the main antenna) On-start on Aux (on startup, use the auxiliary antenna). The options for the RX Diversity parameter should be set, based on the antenna configuration, as follows: Antenna Configuration: A Main and BG Main. RX Diversity: Main only. Antenna Configuration: A Main and A Aux. RX Diversity On-start on Main. Antenna Configuration: BG Main and BG Aux. RX Diversity: On-start on Main. Contact Customer Support (page 14-1) if you have questions about the antenna(s) installed in your HX3.
Frag Thresh	2346	If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of wireless interference. Options are: Any number between 256 bytes and 2346 bytes.
RTS Thresh	2347	If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point. Options are: Any number between 0 and 2347.
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off
Hide Password	On	When On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT (or Blank)	A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.

Parameter	Default	Description
Auth Timeout	8 seconds	Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail. If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed. If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials. Options are: An integer from 3 to 60.
Certs Path	System	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device when not using the Windows certificates store. Ensure the Windows folder path currently exists before assigning the path in this parameter. See Certificates (page 9-32) for instructions on obtaining CA and User Certificates. Options are: none. For example, when the valid certificate is stored as My Computer/System/MYCERTIFICATE.CER, enter System in the Certs Path text box as the Windows folder path.
Ping Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.
Ping Timeout ms	5000	The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout. Options are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a Start Ping button tap. Options are: Any number between 0 and 30000 ms.

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers these choices:

- The Username and Password may be entered on the Credentials screen. If this method is selected, anyone using the device can access the network.
- The Username and Password are left blank on the Credentials screen. When the device attempts to connect to the network, a sign on screen is displayed. The user must enter the Username and Password at that time to authenticate.

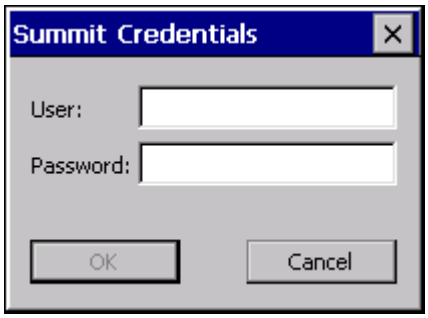
Using Stored Credentials

1. After completing the other entries in the profile, click on the Credentials button.
2. Enter the Username and Password on the Credentials screen and click the OK button.
3. Click the Commit button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
6. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
7. Access the Credentials screen again. Make sure the Validate server and Use MS store check boxes are checked.
8. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
9. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the Browse button.
10. If using EAP FAST and manual PAC provisioning, input the PAC filename and password.
11. Click the OK button then the Commit button.
12. If changes are made to the stored credentials, click Commit to save those changes before making any additional changes to the profile or global parameters.
13. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status tab indicates the device is Authenticated and the method used.

Note: If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed and the user is not prompted to enter valid credentials.

Using a Sign On Screen

1. After completing the other entries in the profile, click on the Credentials button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or LEAP/WPA.
2. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
3. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the Validate server and Use MS store check boxes are checked.
5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the Browse button.
7. Click the OK button then the Commit button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the Username and Password. Click the OK button.



10. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status Tab indicates the device is Authenticated and the method used.
11. The sign-on screen is displayed after a reboot.
12. If a user enters invalid credentials and clicks OK, the device associates but does not authenticate. The user is again prompted to enter credentials.

If the user clicks the Cancel button, the device does not associate. The user is not prompted again for credentials until:

- the device is rebooted,
- the radio is disabled then enabled,
- the Reconnect button on the Diags Tab is clicked or
- the profile is modified and the Commit button is clicked.

Windows Certificate Store vs. Certs Path

Note: It is important that all dates are correct on the HX3 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store.

- To generate the user certificate, see Generating a User Certificate (page 9-36).
- To import the user certificate into the Windows certificate store, see Installing a User Certificate (page 9-41).
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

Root CA certificates are required for EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

Using the Certs Path

1. See Generating a Root CA Certificate (page 9-32) and follow the instructions to download the Root Certificate to a PC.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the Certs Path global variable. Note the location chosen for certificate storage should persist after a reboot.
3. When completing the Credentials screen for the desired authentication, do not check the Use MS store check box after checking the Validate server check box.
4. Enter the certificate name in the CA Cert text box.
5. Click OK to exit the Credentials screen and then Commit to save the profile changes.

Using the Windows Certificate Store

1. See Generating a Root CA Certificate (page 9-32) and follow the instructions to download the Root Certificate to a PC.
2. To import the certificate into the Windows store, See Installing a Root CA Certificate (page 9-35).
3. When completing the Credentials screen for the desired authentication, be sure to check the Use MS store check box after checking the Validate server check box.
4. The default is to use all certificates in the store. If this is OK, skip to the last step.
5. Otherwise, to select a specific certificate click on the Browse (…) button.
6. 

7. Uncheck the Use full trusted store check box.
8. Select the desired certificate and click the Select button to return the selected certificate to the CA Cert text box.
9. Click OK to exit the Credentials screen and then Commit to save the profile changes.

Configuring the Profile

Use the instructions in this section to complete the entries on the Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. See your system administrator for complete information about your network and its wireless security requirements.

To begin the configuration process:

1. On the Main Tab, click the Admin Login button and enter the password.
2. Edit the default profile with the parameters for your network. Select the Default profile from the pull down menu.
3. Make any desired parameter changes as described in the applicable following section determined by network security type and click the Commit button to save the changes.

IMPORTANT – Remember to click the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

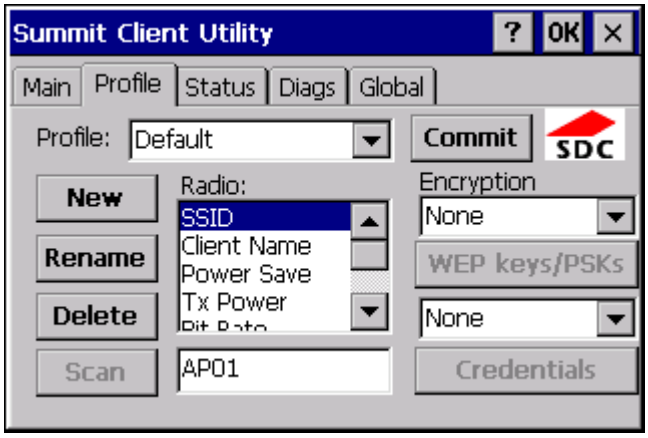
If changes are made to the stored credentials, click Commit to save those changes first before making any additional changes.

No Security

To connect to a wireless network with no security, make sure the following profile options are used.

Enter the SSID of the Access Point assigned to this profile.

4. Set EAP Type to None.
5. Set Encryption to None.
6. Set Auth Type to Open.



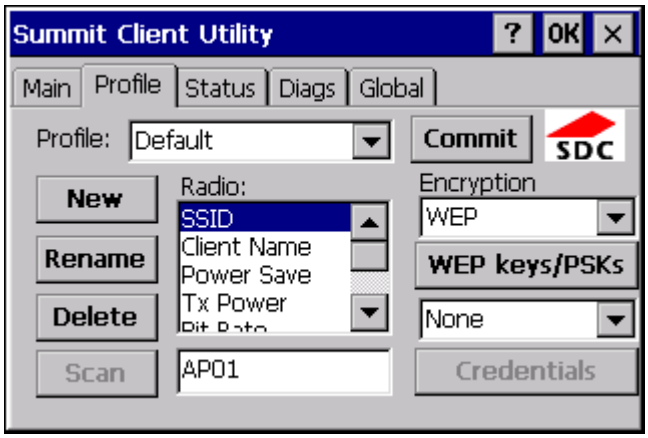
7. Once configured, click the Commit button.
8. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

WEP

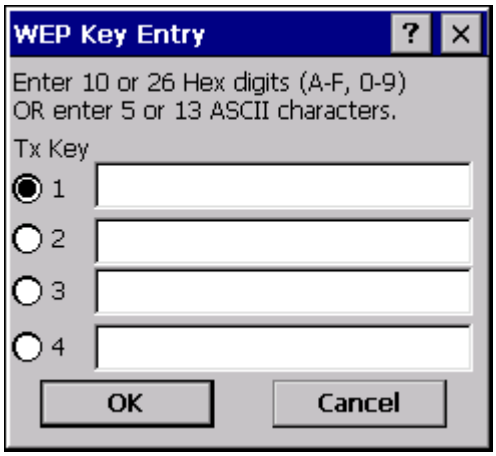
To connect using WEP, make sure the following profile options are used.

Enter the SSID of the Access Point assigned to this profile.

9. Set EAP Type to None.
10. Set Encryption to WEP or Manual WEP (depending on SCU version).
11. Set Auth Type to Open.



12. Click the WEP keys/PSKs button.



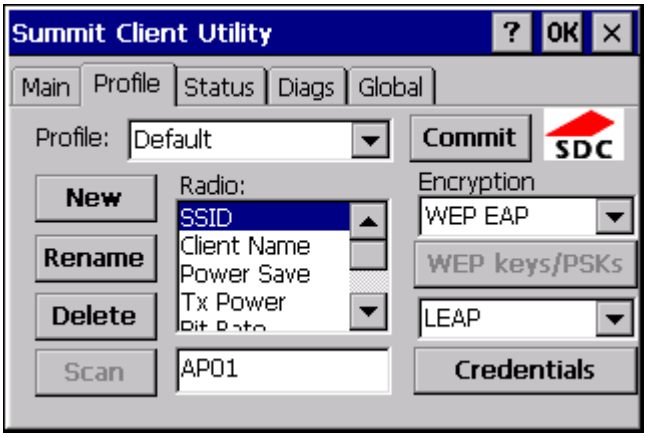
13. Valid keys are 10 hexadecimal or 5 ASCII characters (for 40-bit encryption) or 26 hexadecimal or 13 ASCII characters (for 128-bit encryption). Enter the key(s) and click OK.
14. Once configured, click the Commit button.
15. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

LEAP

To use LEAP (without WPA), make sure the following profile options are used.

Enter the SSID of the Access Point assigned to this profile.

16. Set EAP Type to LEAP.
17. Set Encryption to WEP EAP or Auto WEP (depending on SCU version).
18. Set Auth Type as follows:
    - If the Cisco/CCX certified AP is configured for open authentication, set the Auth Type radio parameter to Open.
    - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to Shared.
    - If the AP is configured for network EAP only, set the Auth Type radio parameter to LEAP.



19. See Sign-On vs. Stored Credentials (page 9-16) for information on entering credentials.
20. To use Stored Credentials, click on the Credentials button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.
21. 

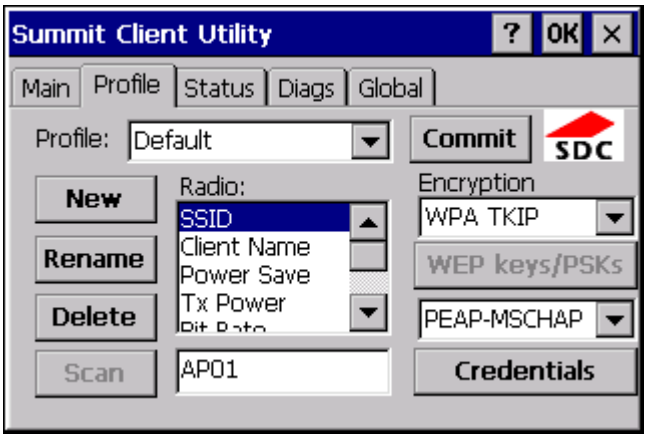
22. Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
23. Enter the password.
24. Click OK then click the Commit button.
25. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/MSCHAP

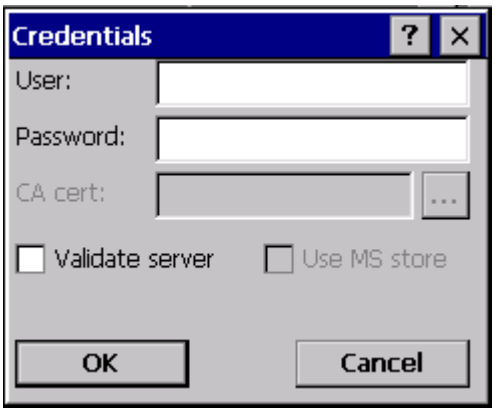
Note: The date must be properly set on the device to authenticate a certificate.

To use PEAP/MSCHAP, make sure the following profile options are used.

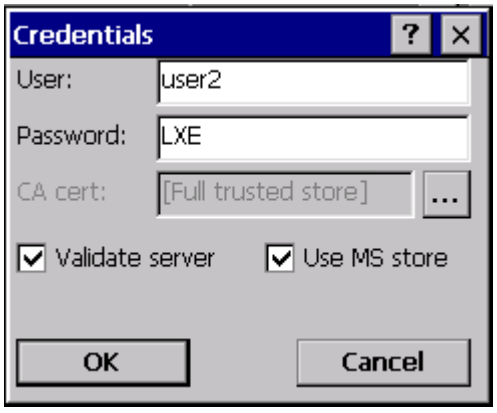
1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to PEAP-MSCHAP.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 9-16) for information on entering credentials.
7. Click the Credentials button.
   - No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
   - For Stored Credentials, User, Password and the CA Certificate Filename must be entered.
8. Enter these items as directed below.



9. Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
10. Enter the password.
11. Leave the CA Certificate File Name blank for now.
12. Click OK then click Commit. Ensure the correct Active profile is selected on the Main Tab.
13. See Windows Certificate Store vs. Certs Path (page 9-18) for more information on certificate storage.
14. Once successfully authenticated, import the CA certificate into the Windows certificate store.

15. Return to the Credentials screen and check the Validate server check box.
16. 

If using the Windows certificate store:

1. Check the Use MS store check box. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the Browse button.
3. Uncheck the Use full trusted store check box.
4. Select the desired certificate and click Select. You are returned to the Credentials screen.

If using the Certs Path option:

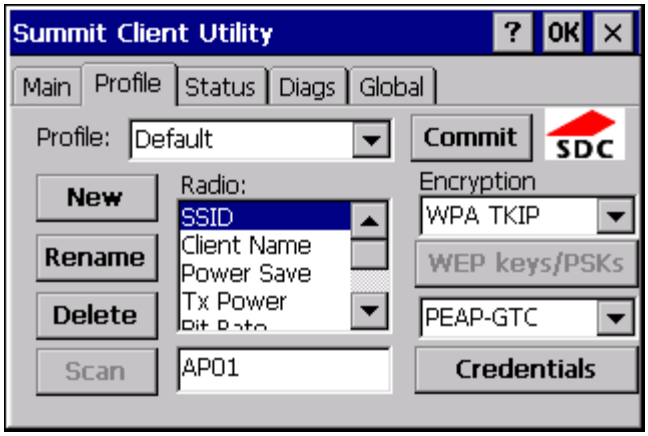
1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Click OK then click Commit.
4. The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.
5. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/GTC

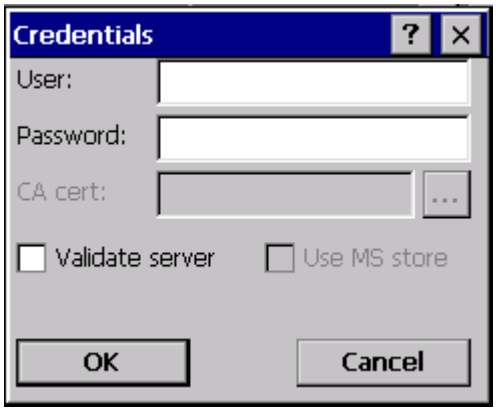
Note: The date must be properly set on the device to authenticate a certificate.

To use PEAP/GTC, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to PEAP-GTC.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



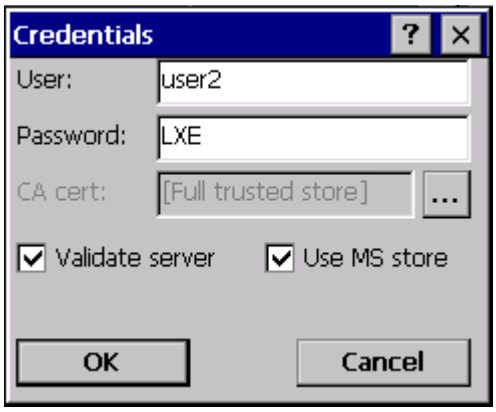
6. See Sign-On vs. Stored Credentials (page 9-16) for information on entering credentials.
7. Click the Credentials button. No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
8. Enter these items as directed below.



9. Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
10. Enter the password.
11. Leave the CA Certificate File Name blank for now.
12. Click OK then click Commit. Ensure the correct Active Profile is selected on the Main Tab.
13. See Windows Certificate Store vs. Certs Path (page 9-18) for more information on certificate storage.
14. Once successfully authenticated, import the CA certificate into the Windows certificate store.

15. Return to the Credentials screen and check the Validate server check box.

Note: Some servers may be configured to allow only a single use of the password for PEAP/GTC. In this case, wait for the token to update with a new password before attempting to validate the server. Then enter the new password, check the Validate Server check box and proceed with the certificate process below.



If using the Windows certificate store:

1. Check the Use MS store check box. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the Browse button.
3. Uncheck the Use full trusted store check box.
4. Select the desired certificate and click Select. You are returned to the Credentials screen.

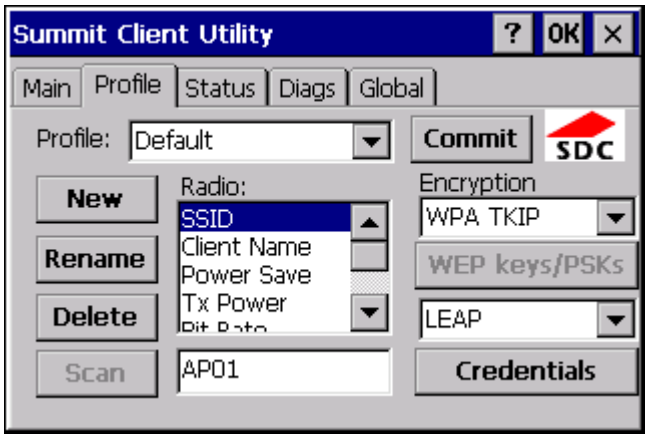
If using the Certs Path option:

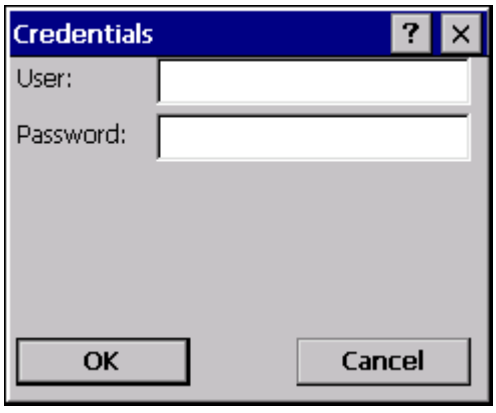
1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Click OK then click Commit.
4. The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.
5. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

WPA/LEAP

To use WPA/LEAP, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to LEAP.
3. Set Encryption to WPA TKIP.
4. Set Auth Type as follows:
   - If the Cisco/CCX certified AP is configured for open authentication, set the Auth Type radio parameter to Open.
   - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to Shared.
   - If the AP is configured for network EAP only, set the Auth Type radio parameter to LEAP.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 9-16) for information on entering credentials.
7. To use Stored Credentials, click on the Credentials button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.
8. 

9. Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
10. Enter the password.
11. Click OK then click the Commit button.
12. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

EAP-FAST

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server. The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the HX3.

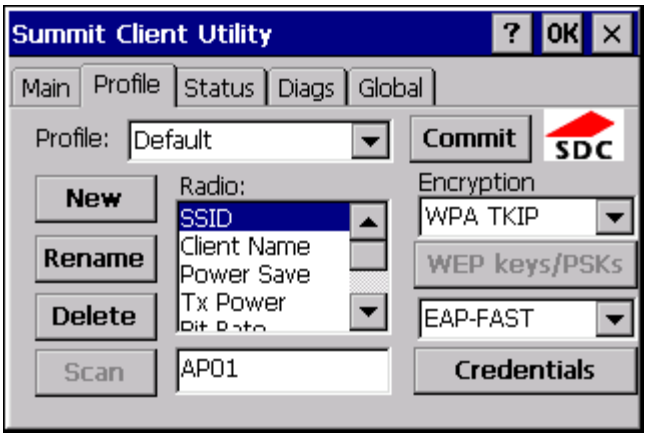
For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the HX3. The same username/password must be used to authenticate each time. See the note below for more details.

Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the \System folder with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

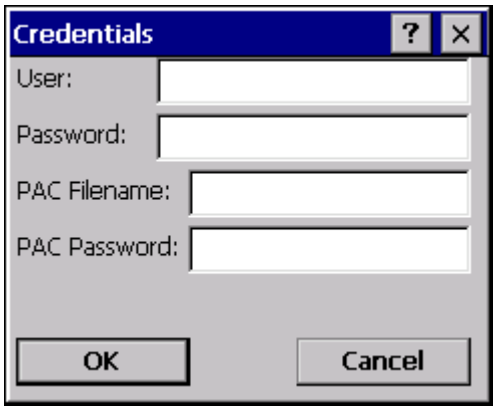
For manual PAC provisioning, the PAC filename and Password must be entered.

To use EAP-FAST, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to EAP-FAST.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 9-16) for information on entering credentials. The entries on the Credentials screen are determined by the type of credentials (stored or sign on) and the type of PAC provisioning (automatic or manual).
7. Click on the Credentials button.
8. To use Stored Credentials, click on the Credentials button. No entries are necessary for Sign-On Credentials with automatic PAC provisioning as the user will be prompted for the Username and Password when connecting to the network.

9. 

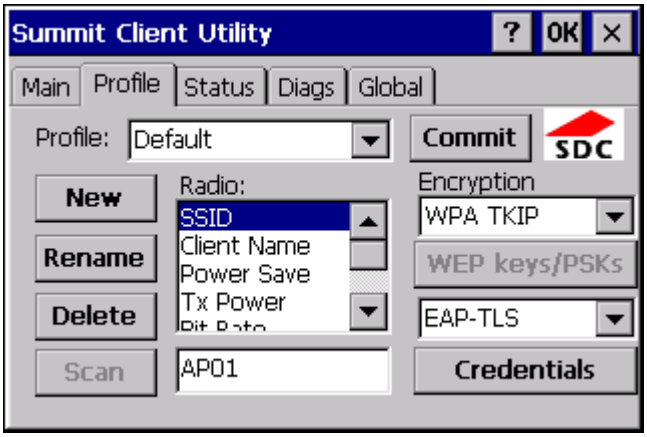
10. To use Sign-On credentials:
    - Do not enter a User and Password as the user will be prompted for the Username and Password when connecting to the network.
11. To use Stored Credentials:
    - Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
    - Enter the password.
12. To use Automatic PAC Provisioning no additional entries are required.
13. To use manual PAC Provisioning:
    - Enter the PAC Filename and PAC Password.
    - The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be read only.
14. Tap OK then click the Commit button.
15. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

EAP-TLS

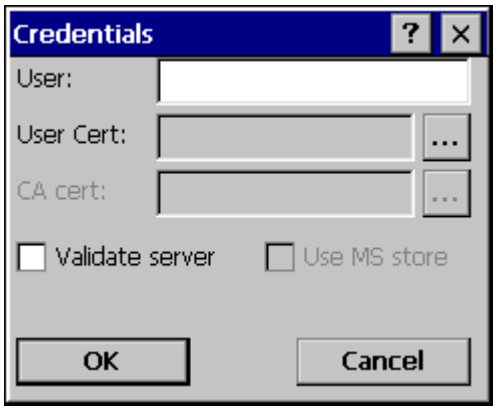
Note: The date must be properly set on the device to authenticate a certificate.

To use EAP-TLS, make sure the following profile options are used.

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to EAP-TLS.
3. Set Encryption to WPA TKIP.
4. Set Auth Type to Open.
5. To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



6. See Sign-On vs. Stored Credentials (page 9-16) for information on entering credentials.
7. Click the Credentials button.
   - No entries except the User Certificate Filename and the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name when connecting to the network.
   - For Stored Credentials, User Certificate Filename and the CA Certificate Filename must be entered.
8. Enter these items as directed below.



9. Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
10. Select a user certificate from the Windows certificate store. Use the Browse button to locate the User Cert from the certificate store. Highlight the desired certificate and press the Select button. The name of the certificate is displayed in the User Cert box.
11. Some versions of the SCU require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.

12. If there are no user certificates in the Windows certificate store, follow these instructions to generate, see Generating a User Certificate (page 9-36), and install the user certificate, see Installing a User Certificate (page 9-41).
13. See Windows Certificate Store vs. Certs Path (page 9-18) for more information on CA certificate storage.
14. Check the Validate server check box.
15. 

If using the Windows certificate store:

1. Check the Use MS store check box. The default is to use the Full Trusted Store.
2. To select an individual certificate, click on the Browse button.
3. Uncheck the Use full trusted store check box.
4. Select the desired certificate and click Select. You are returned to the Credentials screen.

If using the Certs Path option:

1. Leave the Use MS store box unchecked.
2. Enter the certificate filename in the CA Cert text box.
3. Click OK then click Commit.

The HX3 should be authenticating the server certificate and using EAP-TLS for the user authentication.

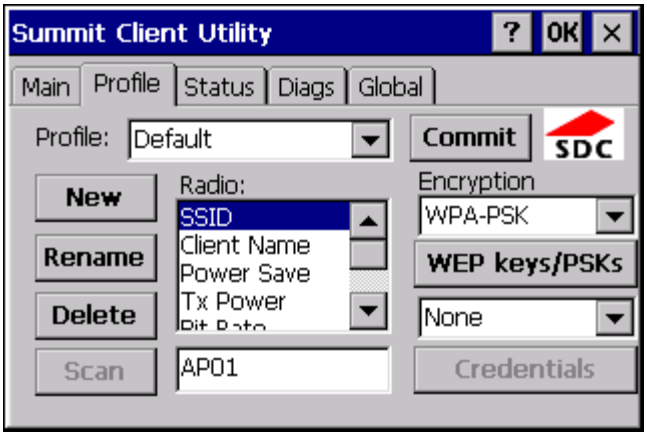
Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

See Certificates (page 9-32) for information on generating a Root CA certificate or a User certificate.

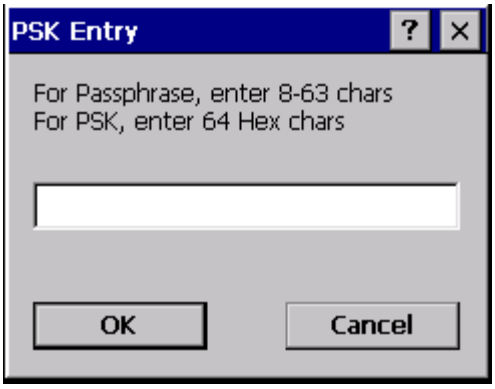
WPA PSK

To connect using WPA/PSK, make sure the following profile options are used:

1. Enter the SSID of the Access Point assigned to this profile.
2. Set EAP Type to None.
3. Set Encryption to WPA PSK or WPA2 PSK.
4. Set Auth Type to Open.



5. Click the WEP keys/PSKs button.



6. This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and click OK.
7. Once configured, click the Commit button.
8. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

Certificates

Note: Refer to the Security Primer (available on the Honeywell web site) to prepare the Authentication Server and Access Point for communication.

Note: It is important that all dates are correct on the HX3 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Root Certificates are necessary for EAP-TLS, PEAP/GTC and PEAP/MSCHAP.

1. See Generating a Root CA Certificate (page 9-32) and download the certificate to a host computer.
2. Connect the HX3 to the a host computer using ActiveSync and copy the certificate to the HX3 \System folder.
3. Install the Root CA Certificate, see Installing a Root CA Certificate (page 9-35).
4. User Certificates are necessary for EAP-TLS.

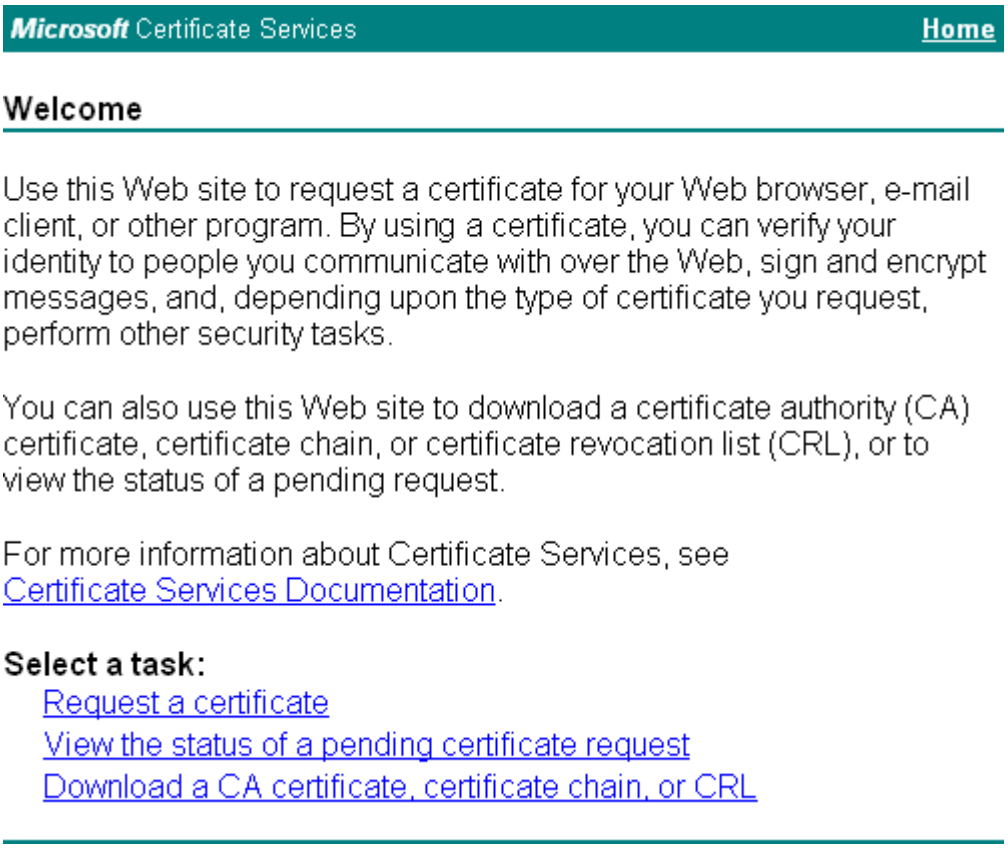
1. See Generating a User Certificate (page 9-36) and download the User Certificate and Private Key file to a host computer.
2. Connect the HX3 to the host computer using ActiveSync and copy the certificate and private key file to the HX3 \System folder.
3. See Installing a User Certificate (page 9-41) and install the User Certificate and Private Key file.
4. After installation, perform a Suspend/Resume.
5. Verify Installation (page 9-44).

Generating a Root CA Certificate

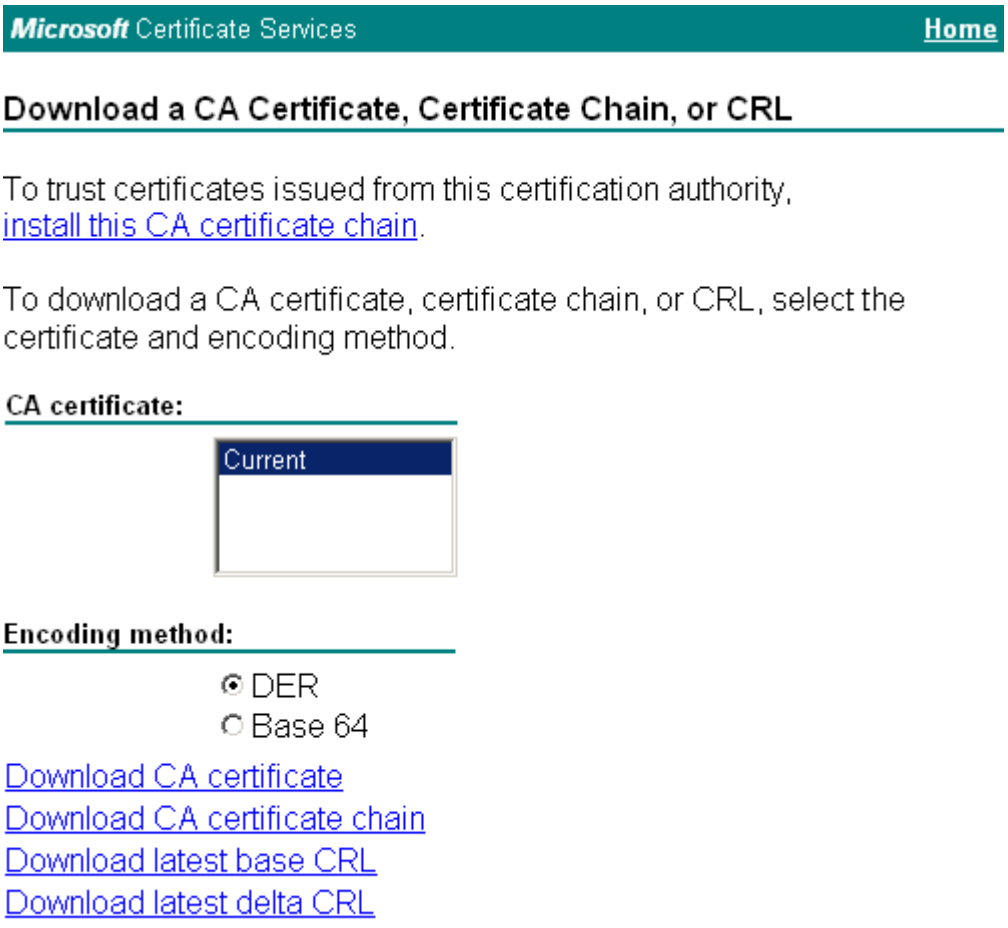
Note: It is important that all dates are correct on the HX3 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

The easiest way to get the root CA certificate is to use a browser on a PC to navigate to the Certificate Authority.

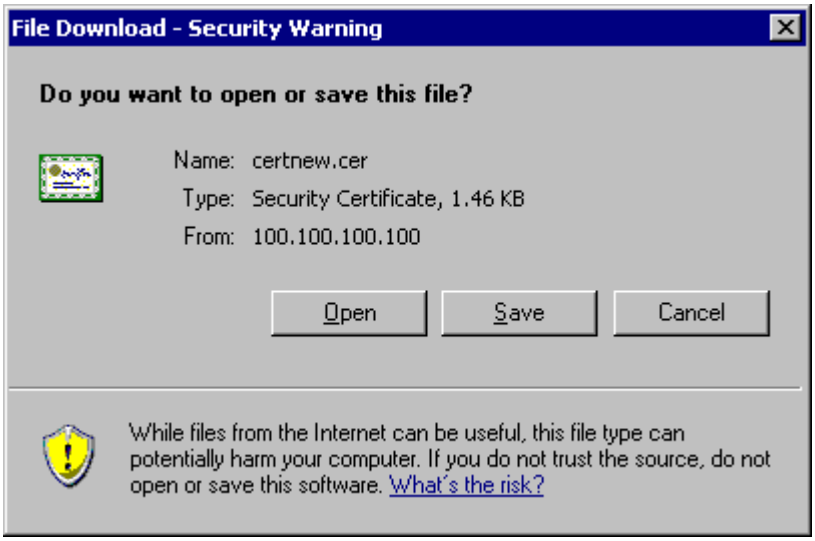
1. To request the root CA certificate, open a browser to http://<CA IP address>/certsrv.
2. Sign into the CA with any valid username and password.



3. Click the Download a CA certificate, certificate chain or CRL link.
4. Make sure the correct root CA certificate is selected in the list box.



5. Click the DER button.
6. To download the CA certificate, click on the Download CA certificate link.



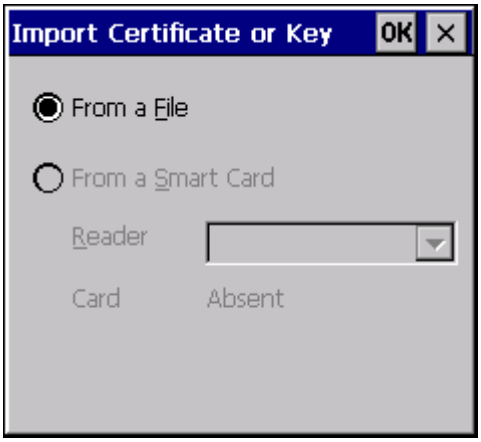
7. Click the Save button and save the certificate. Make sure to keep track of the name and location of the certificate.
8. Install the certificate on the HX3.

Installing a Root CA Certificate

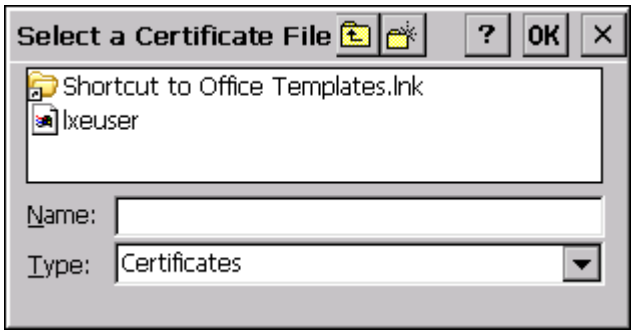
Note: This section is only if the Windows certificate store is used. If the certificate store is not used, copy the certificate to the \System folder or other path specified in the Summit Certs global parameter.

1. Copy the certificate file to the HX3. Import the certificate by navigating to **Start > Control Panel > Certificates.**

2. Tap the **Import** button.



3. Make sure **From a File** is selected and tap **OK**.

4. 

5. Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**.

6. Tap **Yes** to import the certificate.
7. Once the certificate is installed, return to the proper authentication section, earlier in this manual.

Generating a User Certificate

The easiest way to get the user certificate is to use a browser on a PC to navigate to the Certificate Authority.

To request the user certificate, open a browser to http://<CA IP address>/certsrv.

Sign into the CA with the username and password of the person who will be logging into the mobile device.

8. This process saves a user certificate and a separate private key file. Windows CE equipped devices such as the HX3 require the private key to be saved as a separate file rather than including the private key in the user certificate.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

9. Click the **Request a certificate** link.

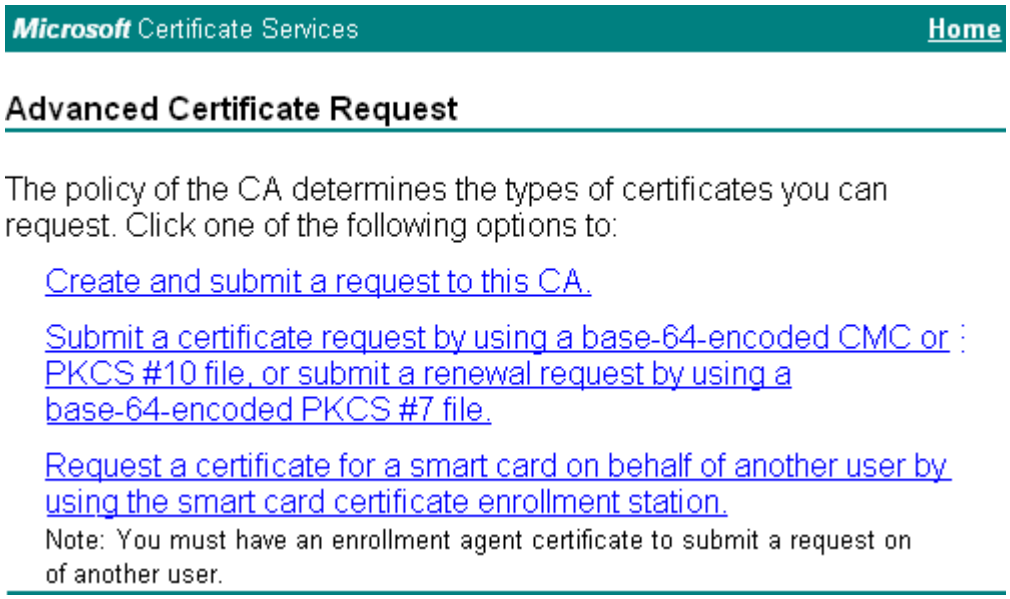
Request a Certificate

Select the certificate type:

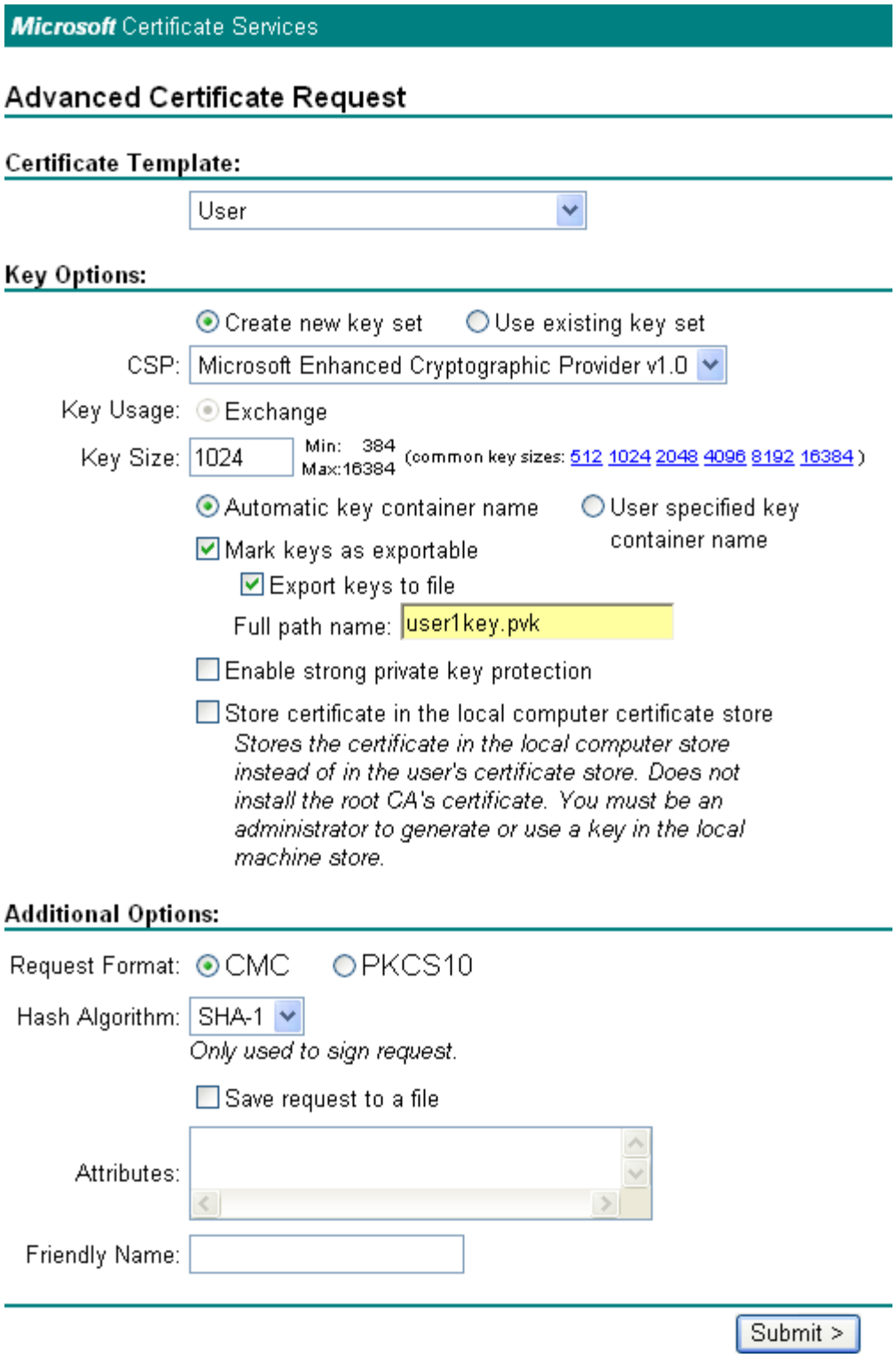
User Certificate

Or, submit an advanced certificate request.

10. Click on the **advanced certificate request** link.

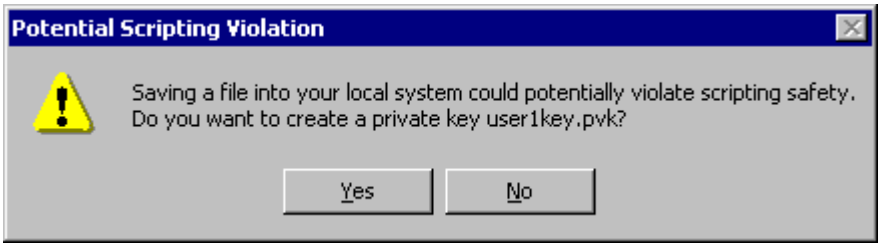


11. Click on the **Create and submit a request to this CA** link.

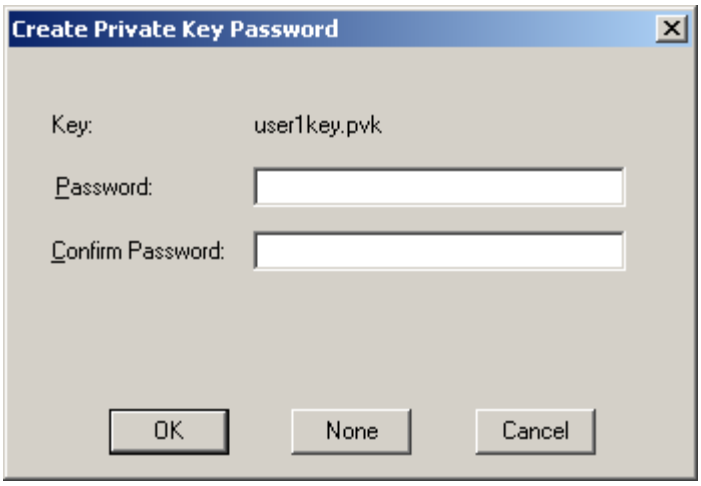


12. For the Certificate Template, select **User**.
13. Check the **Mark keys as exportable** and the **Export keys to file** check boxes.
14. Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.

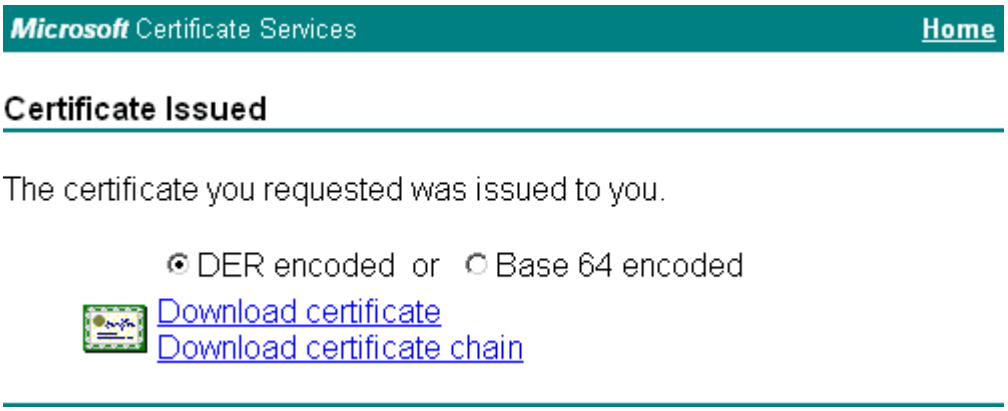
15. Be sure to note the name used for the private key file, for example USER.PVK. The certificate file created later in this process must be given the same name, for example, USER.CER.
16. DO NOT check to use strong private key protection.
17. Make any other desired changes and click the **Submit** button.



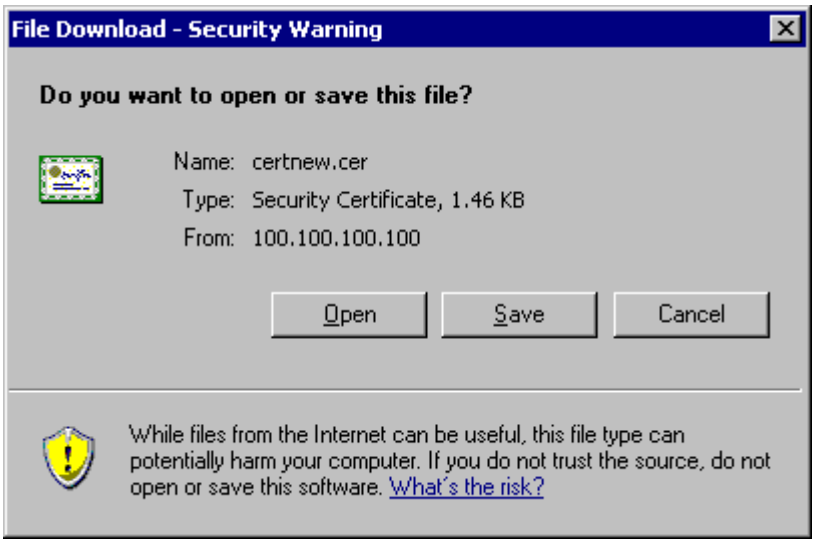
18. If any script notifications occur, click the **Yes** button to continue the certificate request.



19. When prompted for the private key password:
    - Click None if you do not wish to use a password, or
    - Enter and confirm your desired password then click OK.



20. Click the Download certificate link.

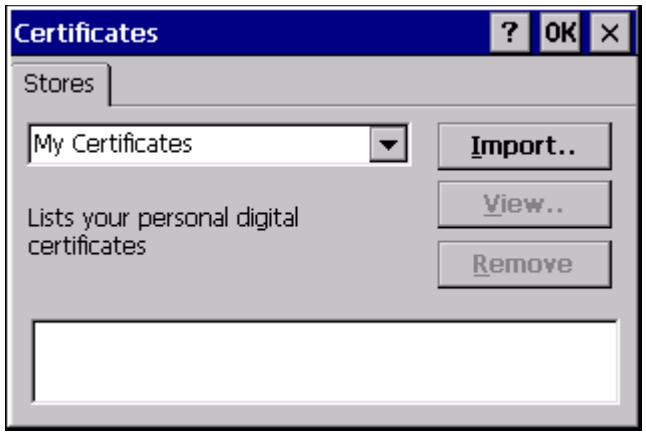


21. Click Save to download and store the user certificate to the PC. Make sure to keep track of the name and location of the certificate. The private key file is also downloaded and saved during this process.
22. Be sure use the same name for the certificate file as was used for the private key file. For example, it the private key was saved as USER.PVK then the certificate file created must be given the same name, for example, USER.CER.
23. Install the user certificate.

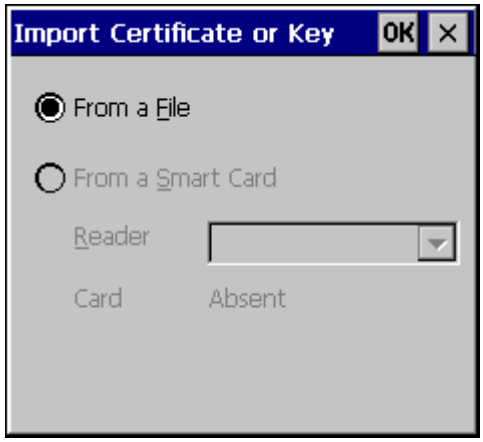
Installing a User Certificate

1. Copy the certificate and private key files to the HX3.
2. Import the certificate by navigating to **Start > Control Panel > Certificates**.

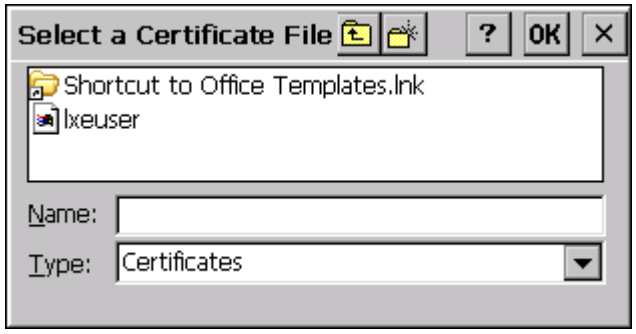
3. Select **My Certificates** from the pull down list.



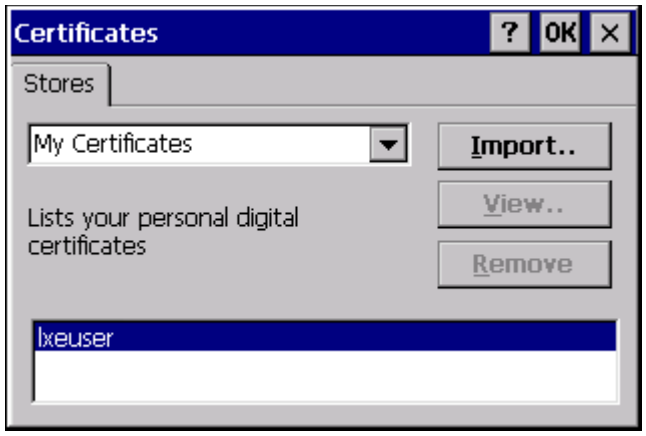
4. Tap the **Import** button.



5. Make sure **From a File** is selected and tap **OK**.



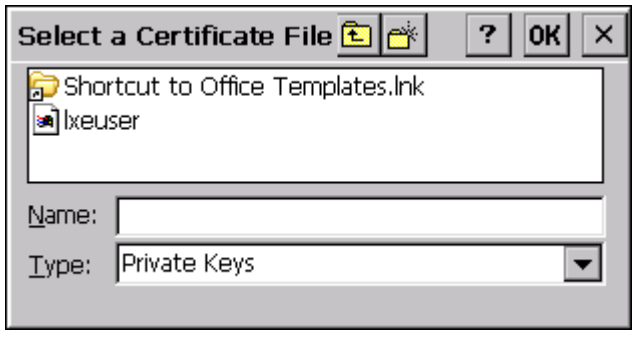
6. Using the explorer buttons, browse to the location where you copied the certificate.
7. Select the certificate desired and tap **OK**.
8. The certificate is now shown in the list.



9. With the certificate you just imported highlighted, tap **View**.
10. From the **Field** pull down menu, select **Private Key**.

- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

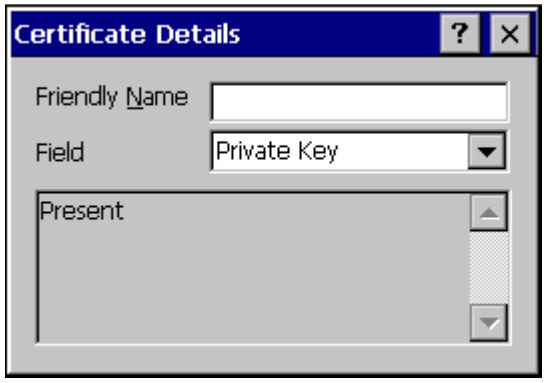
11. To import the private key, tap **OK** to return to the Certificates screen.
12. Tap **import**.



13. Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to **Private Keys,** select the certificate desired and tap **OK**. Enter the password for the certificate if appropriate.

Verify Installation

Tap on View to see the certificate details again.



The private key should now say present. If it does not, there is a problem. Possible items to check:

Note: Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.

Note: Make sure the certificate and private key file have the same name, for example USER.CER for the certificate and USER.PVK for the private key file. If the file names are not the same, rename the private key file and import it again.

10 KeyMap

5 Key Keypad

The HX3 keypad is designed for use with voice applications. Because of the limited design, the HX3 should be connected via ActiveSync to a host computer running LXEConnect when a full keyboard is needed (for example, during system configuration).

To Get this Key Function	Press These Keys in This Order	
Power / Suspend	Power (Red key)	
Volume Up	Blue key	White key
Volume Down	Blue key	Green key
Enter	Yellow key	
Up Arrow	White key	
Down Arrow	Green key	
Blue Mode (Toggle)	Blue key	
Diamond Key	Blue key	Yellow key

11 Desktop Cradle

Unpacking your Cradle

After you open the shipping carton containing the product, take the following steps:

- Check for damage during shipment. Report damage immediately to the carrier who delivered the carton.
- Make sure the items in the carton match your order.
- Save the shipping container for later storage or shipping.

Communication cables and power cables are ordered separately.

Introduction

This chapter provides instruction for the end-user, installer or system administrator to follow when setting up or using the desktop cradle.

Note: The HX2 and HX3 use the same HX2 labeled desktop cradle. Batteries used by the HX3 body worn Voice device can be charged and recharged in the HX2 labeled Desktop Cradle.

The desktop cradle is designed to:

- secure the HX3 with or without a rubber boot,
- recharge a tethered HX3 battery and a spare battery (both charging bays accept Standard and Extended batteries),
- provide storage for the tethered Ring Scanner when the HX3 is docked,
- and enable serial communication with USB devices (host, client, and other USB cabled devices).

The HX3 cradle is available with or without a power cord. If ordered without a power cord, a C14 style power cord is required. Communications cables for the HX3 are available separately.

Using an external power supply, the desktop cradle recharges Standard batteries in approximately 4 hours (8 hours for the Extended battery). The HX3 does not need to be docked in the cradle during a spare battery charging process. Tethered battery recharging is performed using one of the battery bays located behind a docked HX3. The tethered battery can remain tethered to the HX3 while the HX3 is docked.

HX3 keypad data entries can be mixed with ring scanner bar code data entries while the HX3 is docked in the cradle. The HX3 can be either On or in Suspend Mode while in the cradle. Power must be applied to the cradle before any battery bay or docking bay charging can commence.

Wireless host/client communications can occur when the cradle is receiving external power and the HX3 is docked in a powered cradle. Wireless functions draw power from external power when the HX3 is docked. Cradle communication and power cables are available from Honeywell.

As soon as the HX3 is docked in a powered cradle, power connection between the tethered battery and the HX3 stops. The HX3 is now receiving power through the powered cradle connector. The HX3 backup battery starts trickle-charging. If the tethered battery is placed in a charging bay, the tethered battery starts re-charging.

The desktop cradle is not certified for use in Hazardous Locations. The desktop cradle cannot support USB or RS232 tethered scanners.

Preparing the Desktop Cradle for Use

Note: Keep dirt and foreign objects out of the cradle. Do not short circuit any of the charging terminals (pins), as this action could result in injury or property damage.

Place the desktop cradle on a stable surface out of the way of:

- inclement weather,
- extremely high concentrations of dust or wind blown debris,
- accidental knocks, bumps or other shocks to the cradle and items in the cradle bays.
- Leave enough space at cable connectors to ensure cables are protected from jostling, tugging or being disconnected by passing objects.
- Getting Started

The following list outlines, in a general way, the process to follow when preparing the desktop cradle for use. Refer to the following sections in this document for more details.

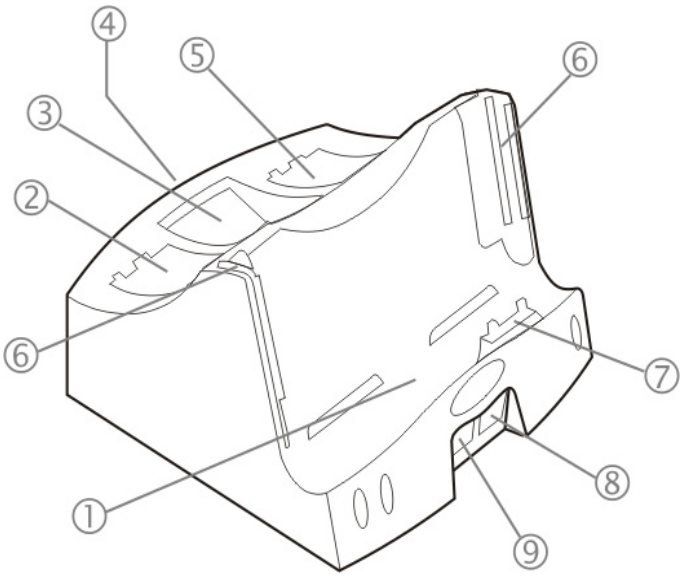
Do not place the HX3, batteries or ring scanner into the cradle bays until the cradle is on a stable, horizontal surface.

1. Prepare the cradle for use. See Preparing the Desktop Cradle for Use (page 11-1).
2. Connect the external power cable to a dependable power supply.
3. Connect the cradle end of the power cable to the power port on the back of the cradle.
4. The B1 and B2 LEDs flash yellow-red-green then go out. The empty powered cradle is ready for use.
5. Prepare the HX3 for docking by removing it from the arm band, hip-flip or audio case, if used.
6. Insert the HX3 in the Docking Bay.
7. Insert the tethered battery in one of the battery charging bays at the back of the cradle. The battery can remain tethered as the power connection between the battery and the HX3 is broken as soon as the HX3 connects to the power source via the cradle-power connector.
8. Dock the Ring Scanner, if attached, in the Ring Scanner bay (located between the battery charging bays).
9. Insert a spare battery in the remaining battery charging bay at the back of the cradle, if desired.
10. The B1 and B2 LEDs illuminate as soon as a battery is inserted in a charging bay.
11. Connect USB cables at the front of the cradle, if desired.
12. Press the Power button on the HX3. The cradle PWR LED illuminates. The fully loaded cradle is ready for use.

Extreme ambient temperatures may have unexpected / undesired effects on the HX3, ring scanner, cradle and batteries in the charging bays. Refer to Technical Specifications (page 13-1) for recommended temperature ranges for daily operation, battery charging and storage.

Components

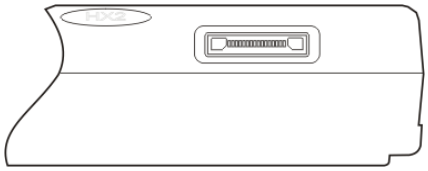
Front View



1. HX3 Docking Bay
2. Left Battery Charging Bay
3. Tethered Ring Scanner Storage
4. Back Connectors - AC Power Port and RS232 Serial Port
5. Right Battery Charging Bay
6. Cradle Side Rails
7. HX2 Cradle Connector (power and I/O)
8. USB Port (USB-B Client)
9. USB Port (USB-A Host)

Note: 1Either battery charging bay can charge stand-alone or tethered Standard and Extended batteries.

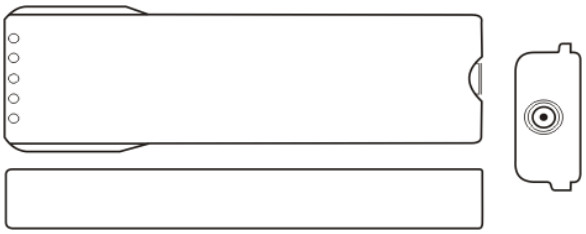
Bottom View



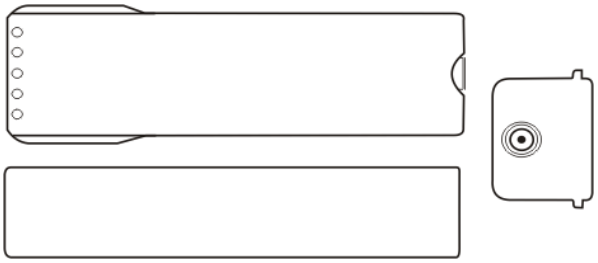
The HX3 Cradle Connector is located on the bottom of device.

Rechargeable Lithium Ion Battery Pack

Each battery pack has one side alignment rib wider than the other to ensure the battery pack is inserted in the battery charging bay easily. This design ensures the battery charging terminals line up with the charging terminals in each charging bay.



Standard Battery

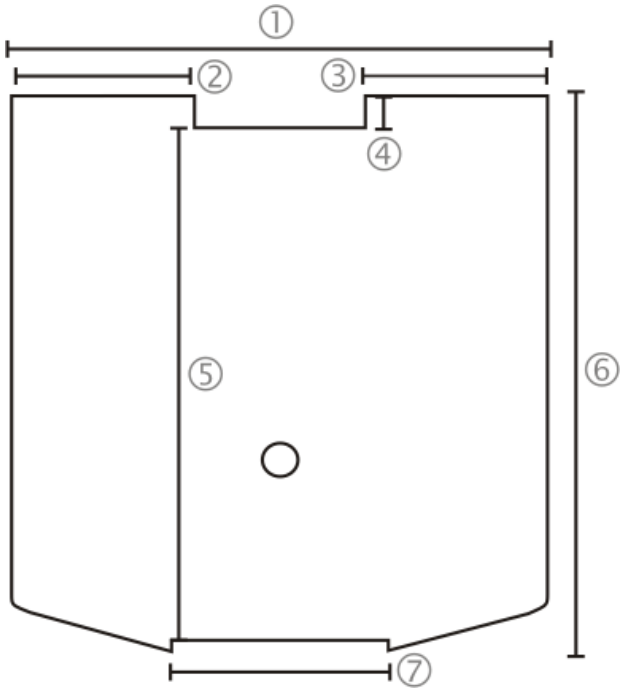


Extended Battery

Note: When a battery pack is not in use, lay the battery pack contact-side up in a protected environment. When feasible, protect the battery from ESD and contamination. Any dust or moisture that adheres to the tether connector can potentially cause damage upon cable re-connection.

Battery Charge Contact	Description	Pin
Power (+)	Positive terminal	1
ID (D)	Battery ID	2
Voltage Sense (S)	Cell voltage sensor	3
Thermistor (T)	Temperature sensor	4
Ground (-)	Negative terminal	5

Desktop Cradle Footprint



Bottom View – Measurements are Not to Scale

Approximations

1. 5.5 in / 14 cm
2. 2.0 in / 5.1 cm
3. 2.0 in / 5.1 cm
4. 0.45 in / 1.14 cm
5. 5.5 in / 14 cm
6. 6.0 in / 15.2 cm
7. 2.5 in / 6.3 cm

Cradle Height: 3.4 in / 8.6 cm
Cradle Width: 4.75 in / 12.1 cm
Cradle w/Tethered Battery Height: 6 in / 15 cm

Table Mounting

The cradle can be mounted to a flat, stable surface using the <1mm hole in the Tethered Ring Scanner storage bay (fasteners, screwdrivers, etc., not supplied).

Periodically check the connection and re-tighten if necessary.

Power Cable

Important: Use the power cable provided with the cradle's power supply adapter with the desktop cradle only.

There are two types of external power supplies for the cradle:

- Power Supply, External, AC, US (with power cable)
- Power Supply, External AC, International (without power cable)

The external power supply may be connected to either a 120V, 60Hz supply or, outside North America, to a 230V, 50Hz supply, using the appropriate detachable cord set.

In both cases, connect the external power supply 2-prong end to a source of power provided with maximum 15 Amp over current protection (10 Amp for 230V circuits).

1. Firmly press the cradle end (L-shaped 5mm barrel connector) of the power cable into the power connector on the back of the cradle.
2. Firmly press the C8-2 female end of the power cable into the two male connector pins on the power adapter, guided by the connection notches on the top and bottom.
3. Plug the 2-prong end of the cable into any AC wall outlet with a dependable power source. AC power is now being supplied to the AC/DC power adapter and the cradle.

Each time the HX3 is docked in the powered cradle, the connection between the tethered battery and the HX3 terminates.

Press the Power button on the HX3 and the PWR LED on the cradle will illuminate.

When a battery is in either one (or both) of the battery charging bays, the battery charging bay LED (B1 / B2) is illuminated.

Connecting Input/Output Cables

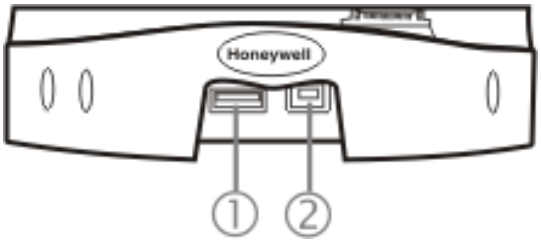
Route all cables to ensure they are protected from jostling, tugging or being disconnected by passing objects.

The cradle must be receiving power from an external power source before HX3 battery charging can begin.

USB Cable

The cradle provides 5V to the USB Host connector (0.5A) to allow interfacing with an external USB keyboard or USB pointing device through the cradle. USB Client connections do not receive power through the cradle.

The USB ports are located on the front of the desktop cradle.



Requires Cable Type:

- USB A Host e.g., scanner
- USB B Client e.g., Activesync cable

1. Ensure there is a stable source of power applied to the USB external device.
2. Turn the device On.
3. Connect the USB-A (Host - left connector) or USB-B (Client - right connector) plug to the appropriate receptacle at the bottom front of the desktop cradle.
4. USB connected external device and HX3 communication is available.

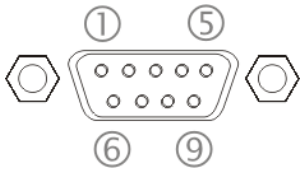
Serial Cable

Note: Only approved Honeywell cables are to be used for serial communication between the cradle and external devices.

Note: The serial cable port is located on the back of the desktop cradle.

Note: Assemble the AC Adapter and connect it to the desktop cradle. Verify the cradle has a dependable power source.

5. Connect a female DB9 connector to the male DB9 serial port on the back of the desktop cradle. The connection should be finger tight.
6. The DB9M cradle connector provides limited RS232 functionality, as the following pinout table shows.

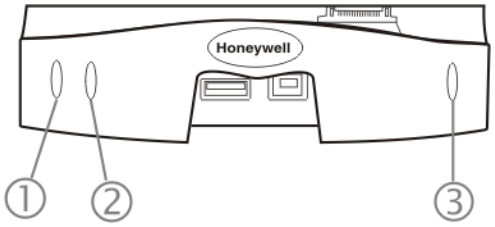


Pin	Signal
1	Not Connected
2	RXD
3	TXD
4	Not Connected
5	Ground
6	Not Connected
7	RTS
8	CTS
9	Not Connected

Note: Pin 9 of this port does not have power capability. The desktop cradle can not support tethered scanners.

Indicators

The LEDs may flicker between green, amber and red upon the cradle first receiving external power. This is normal. The cradle is performing a self-check and upon completion, the LEDs will return to their normal state (see below).



1	B1 LED – Back left battery charging bay	Normal State – Off. With battery and AC power, normal state may be any state listed in Cradle LEDs.
2	PWR LED - HX3 docked / on / receiving power bay	Normal State – Off. With HX3 in, turned On and AC power, normal state is On.
3	B2 LED – Back right battery charging bay	Normal State – Off. With battery and AC power, normal state may be any state listed in Cradle LEDs.

Cradle PWR LED

When PWR LED is …	It means ….
Off	No AC/DC power supplied to the cradle and/or No HX3 in the charging bay and/or HX3 is not properly seated in charging bay and/or if this is the first time the HX3 has been inserted, the HX3 is properly seated and has not been powered On.
Green	HX3 is On, is properly seated in the charging bay and is receiving external power through the cradle.

B1 and B2 LED

When B1 and/or B2 LED is …		It means ….
Off	No battery or no AC power	No spare battery in the battery bay(s) or no AC/DC power is being applied to the cradle.
Green	Charged	Spare battery pack fully charged.
Red	Charging	Spare battery pack charging.
Amber	Standby	Spare battery pack temperature out of range.
Flashing Red	Fault	Spare battery pack fault or failure.

Docking and Undocking the HX3

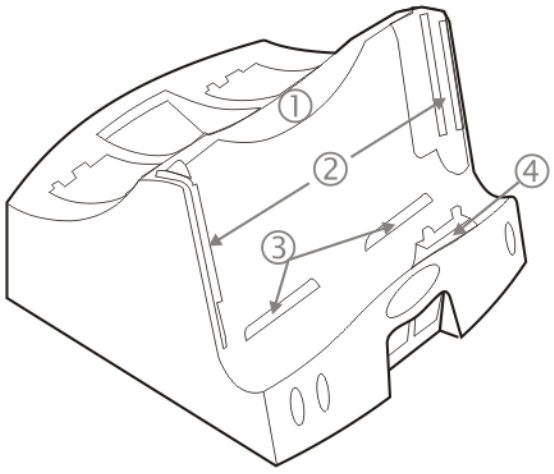
The HX2 cradle docking bay can accommodate an HX3 with or without a rubber boot.

Remove the hip flip, arm band or voice case if used.

The HX3 is inserted in the cradle with the keypad visible and available for use.

The HX3 can be inserted and removed with one hand, or if preferred, two hands.

Do not "slam" or slide the HX3 sideways into the cradle. Do not rock the HX3 forward out of the cradle. Damage may result.



1. Fingertip Depression
2. Side Rails
3. Bottom Rails
4. Cradle power supply connector for a docked HX3

Docking the HX3

1. Prepare the HX3 for docking by removing it from the armband, hip flip or voice case if used. Place the wearable accessories in a clean, safe location.
2. Slide the HX3 armband brackets straight down into the side rails on either side of the docking bay, making sure the cradle connector on the HX3 and the cradle connector in the docking bay line up.
3. Press the HX3 down firmly until both connectors “click” together.
4. When the HX3 is properly seated in the docking bay, tap the Power button on the HX3. The PWR LED on the cradle illuminates if the HX3 is properly seated in the cradle. If the cradle PWR LED does not illuminate, remove the HX3 from the bay and reinsert.
5. Place the tethered battery, if any, in a battery charging bay. Battery charging commences. The battery does not need to be disconnected from the HX3, if desired.
6. Place the tethered Ring Scanner, if any, in the Ring Scanner bay. The Ring Scanner does not need to be disconnected from the HX3.
7. The docked HX3 is ready to use AC power for communication and backup battery recharging.

Undocking the HX3

Important: Do not put pressure on the HX3 display when removing the HX3 from the cradle.

1. Hold the HX3 firmly, and brace your thumb on or under the logo (just above the HX3 display). *Hint: Pushing down with your fingertips in the fingertip depression (behind the HX3) at the same time may be helpful.*
2. Pull the HX3 straight up to disconnect the cradle connector on the HX3 from the cradle connector in the docking bay.
3. If the ring scanner and battery were tethered to the HX3 while it was docked, they remain tethered when the HX3 is removed from the cradle.
4. Reconnect the HX3 wearable device to the armband, voice case or hip flip, sliding the HX3 battery into the battery sleeve.

Note: The <1mm hole in the Tethered Ring Scanner storage bay is used to guide the fastener (screw) when attaching the desktop cradle to a flat, stable surface (fasteners, screwdrivers, etc., not supplied by Honeywell).

Docked HX3 Mode States

When the HX3 is not docked in a powered cradle it can be set to enter Suspend Mode using **Start > Settings > Control Panel > Power > Schemes** tab.

When the HX3 is docked in a powered cradle it can be placed in Suspend Mode by tapping the Power key.

Switch State to Suspend Mode established in **Start > Settings > Control Panel > Power > Schemes** tab is not available until the HX3 is disconnected from the cradle.

Pre-existing User Idle and System Idle function as scheduled when the HX3 is docked in a powered cradle.

IMPORTANT

- Do not put the HX3 into Suspend Mode (by tapping the Power key) while the HX3 is connected to peripheral devices (or ActiveSync) through the connectors on the desktop cradle. The HX3 is unable to maintain the connection during Suspend Mode.
- If the USB connections are interrupted due to a Suspend operation – when the HX3 resumes, disconnect the cables and then reconnect the cables again to initiate USB and/or ActiveSync connection again.

Ring Scanner Storage

If Ring Scanning is required while the HX3 is receiving power through the desktop cradle, the AC Adapter should be assembled and attached to the desktop cradle first.

The Ring Scanner can be placed in the depression between the battery charging bays while tethered to an HX3 in the Docking bay.

The Ring Scanner depression can also be used to store an untethered ring scanner. The depression does not have a connector.

Inserting and Removing a Tethered Battery

Prerequisites:

- The AC adapter has been assembled and attached to the desktop cradle. Batteries can not charge in an unpowered desktop cradle.
- The HX3 tethered battery has been removed from the armband or hip-flip battery sleeve or battery bracket.

Do not drop or slam the HX3 battery into the charging pocket. Damage may result.

A fully depleted Standard battery recharges fully in approximately four hours in a powered cradle charging pocket.

A fully depleted Extended battery recharges fully in approximately eight hours in a powered cradle charging pocket.

The HX3 tether connector must be at the top of the battery in the charging bay. The battery will not fit properly into the charging pocket if the tether connector is inserted into the depression of the charging bay.

Each charging pocket can recharge either battery – standard or extended. The extended battery is noticeably thicker than the standard battery.

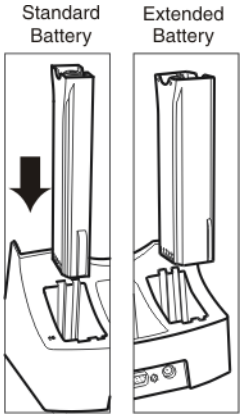
Make sure the battery terminals line up with the charging terminals in the charging bay.

Inserting a Tethered Battery into the Charging Bay

Grasp the battery, not the tether, and ensure the battery terminals line up with the charger terminals in the charging pocket. Slide the battery straight down into the charging pocket until the charging terminals meet.

The charging pocket LED illuminates.

See Indicators (page 11-6) to determine the status of the B1 or B2 charging pocket LED.



Removing a Tethered Battery from the Charging Bay

Grasp the battery, not the tether, and pull the battery straight up and out of the charging pocket.

The charging pocket LED (B1 or B2) turns off.

Cradle Help

Issue:

Battery LED is Amber (Standby)

Solution:

The cradle can wait up to two hours for the battery pack temperature to return to an acceptable temperature range when the charging process will commence. Battery packs can only be charged when their temperature is between 10°C (50°F) and 40°C (104°F).

Issue:

Battery LED is flashing red (Fault)

Solution:

Battery pack fault or failure. Contact Customer Support (page 14-1) for help.

Maintenance

Inspect the rubber feet and replace them if missing, broken or cracked. Check the cradle regularly for excessive wear at pressure points. If the cradle is mounted to a stable surface, check surface mounting connections periodically and re-tighten as necessary.

If the cradle becomes cracked or broken at any time, it must be taken out of service and replaced. Contact Customer Support (page 14-1) for a replacement cradle.

There are no serviceable parts in the desktop cradle. Do not attempt to open the unit.

Cleaning

Do not use paper towels or harsh-chemical-based cleaning fluids since they may result in damage to the surfaces and/or battery charging terminals (pins).

Use a clean soft cloth to wipe any dirt, moisture or grease from the HX3, spare battery packs, charging contacts (pins) or the cradle.

Do not use any liquid to clean the battery pack, HX3, cradle, or charging pockets. Spray or dampen the cleaning cloth with liquids/sprays. If possible, clean only those areas which are soiled.

Lint/particulates can be removed from the connectors, charging terminals and charging/docking pockets with clean, filtered canned air.

12 Battery Charger

Unpacking your Battery Charger

After you open the shipping carton containing the product, take the following steps:

- Check for damage during shipment. Report damage immediately to the carrier who delivered the carton.
- Make sure the items in the carton match your order.
- Save the shipping container for later storage or shipping.

Introduction

The Battery Charger is designed to simultaneously charge six rechargeable Lithium Ion (Li-Ion) battery packs. The time required for charging is dependent upon the battery pack temperature and conditions.

The battery charger should be located in an area where it:

Is well ventilated.

- Is not in high traffic areas.
- Locates or orients the AC cord so that it will not be stepped on, tripped over or subjected to damage or stress.
- Has enough clearance to allow easy access to the power port on the back of the device.
- Is protected from rain, dust, direct sunlight or inclement weather.

This device is intended for indoor use only and requires an indoor AC power source. The charger is not approved for use in Hazardous Locations.

This device cannot charge/recharge coin cell batteries sealed inside the HX3, if any.

Note: The HX2 and HX3 use the same batteries. Batteries used by the HX3 body worn Voice device are charged, recharged and analyzed in the HX2 labeled battery charger.

Note: This chapter is intended to familiarize the user with the safety and operating instructions necessary to use the Battery Charger (Model HX2A310CHGR6US, HX2A311CHGR6WW) to charge rechargeable lithium-ion battery packs (HX2A301BATTSTD, HX2A302BATTEXT).

This guide should be readily available to all users and maintenance personnel using this battery charger.

Cautions and Warnings

Battery Charger

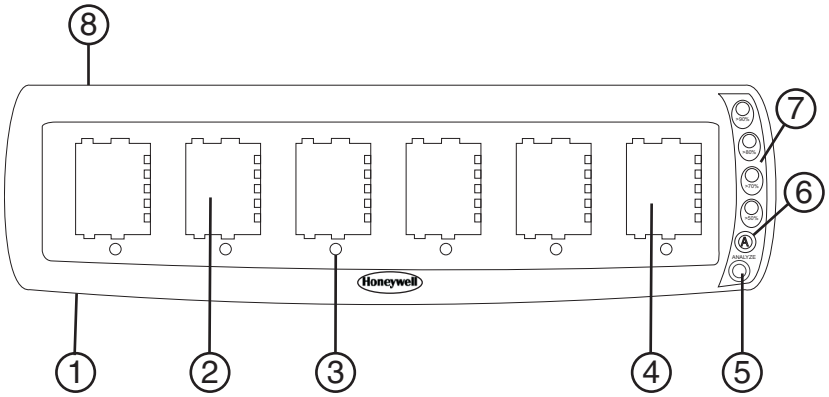
- There is a risk of explosion if the HX3 Li-Ion battery in the charging pocket is replaced by an incorrect type. Other batteries or battery packs may burst causing injury or property damage.
- Do not insert any other type of Li-Ion battery in the HX3 battery charging pocket.
- Do not allow cleaning agents of any kind to contact the battery charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.
- Disconnect the charger from AC power by pulling the plug; not the cord.
- Use care when inserting battery. Do not “slam” or slide the battery into the pocket, this could damage the charger.
- Keep dirt and foreign objects out of the battery pocket. Do not short circuit any of the contacts in the battery pocket, this could result in injury or property damage.
- Do not disassemble or perform modifications to the charger. There are no user serviceable components in the charger.

Lithium-Ion Battery Pack

- Dispose of used Li-Ion batteries according to the instructions for the type of battery.
- When not in use, lay the battery pack contact-side up in a protected environment.
- Do not store the Li-Ion battery pack in direct sunlight or anywhere the battery pack cannot cool down.
- If the Li-Ion battery pack is hot after removal from the HX3, allow it to cool at room temperature or in a cool air stream before placing it in the charger.
- Do not dispose of Li-Ion batteries into a fire. Burning will generate hazardous vapors and may cause the battery to explode. Failure to observe this warning may result in injury from inhalation of vapors or burns from flying debris.
- Do not immerse Li-Ion batteries in water or any other liquid. If batteries are immersed, contact Honeywell.
- Do not disassemble or perform modifications to the battery. There are no user serviceable components in the battery.
- Do not place the Li-Ion battery into a pocket or toolbox with conductive objects (coins, keys, tools, etc.). A Li-Ion battery placed on damp ground or grass could be electrically shorted.
- Do not store Li-Ion batteries above 140°F (60°C) for extended periods.
- Failure to observe these warnings could result in injury or damage to the battery from rapid discharge of energy or battery overheating.
- Electrolyte Burns. Be careful when handling batteries. If a battery is broken or shows signs of leakage do not attempt to charge it. Dispose of it! Lead and Nickel-based cells contain a chemical solution that burns skin, eyes, etc. Leakage from cells is the only possible way for such exposure to occur. In this event, rinse the affected area thoroughly with water. If the solution contacts the eyes, get immediate medical attention.
- Electrical Burns. Batteries are capable of delivering high currents when accidentally shorted. Accidental shorting can occur when contact is made with jewelry, metal surfaces, conductive tools, etc., making the objects very hot. Never place a charged battery in a pocket or case with keys, coins, or other metal objects.

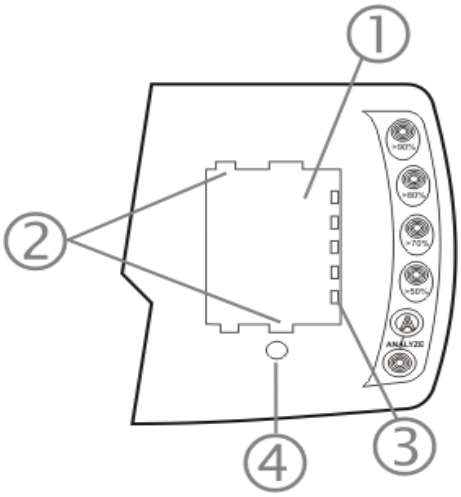
Components

Battery Charger



1. Front
2. Battery Charging Pocket
3. Battery Charge LED Indicator
4. Analyze Pocket
5. Analyze LED
6. Analyze Dome Switch
7. Analyze Progress LEDs
8. AC/DC Power Connector

Battery Charging Pocket



1. Battery Charging Pocket
2. Alignment Ribs
3. Battery Charging Contacts
4. Battery Charge Progress LED

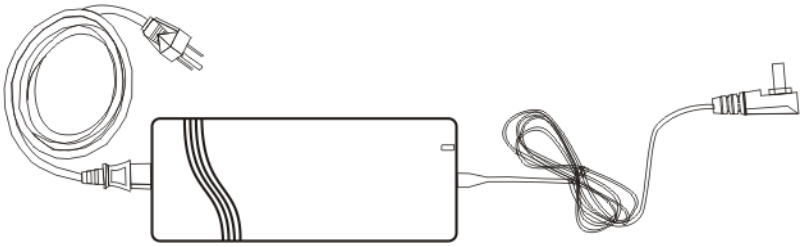
Installation

Assemble the Power Supply

Note: Assemble the AC adapter for the Battery Charger before connecting it to the charger.

The AC power supply for the battery charger is shipped with the battery charger unless you require a country-specific power supply and cable assembly.

The battery charger power supply is intended for use with the battery charger only.



1. Plug the 3-prong end of the cable into an AC wall outlet.
2. Firmly press the female end of the power cable into the male connector on the AC power adapter. An LED on the power adapter illuminates when AC power is available.
3. AC power is now being applied to the power adapter.

Setup

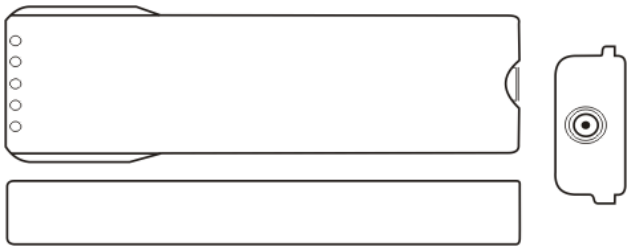
Prerequisite: The AC Adapter is assembled and receiving AC power.

Place the battery charger on a flat, horizontal, hard surface or fasten securely to a stable surface using the keyhole openings on the bottom of the battery charger.

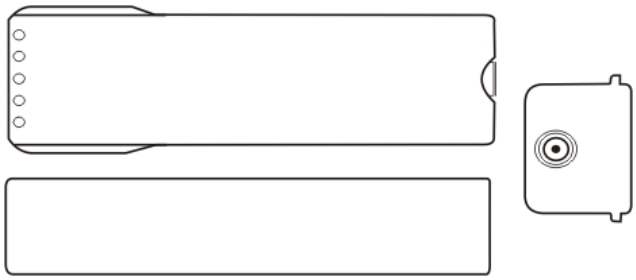
Do not insert battery packs until the battery charger has finished powering up:

- Insert the power connector into the power outlet at the back of the battery charger.
- AC power is now being applied to the battery charger and it begins to power up.
- Charge pocket LEDs flash while the battery charger enters and exits the startup check.
- When the charge pocket LEDs are not illuminated, the battery charger is ready for use.

Charging Batteries



Standard Battery - 2000mAh



Extended Battery - 4000mAh

New batteries should be charged fully before first use. The life and capacity of a Lithium Ion battery pack can vary significantly depending on the discharge current and the environment in which it is used.

Use the charge function to return the HX3 battery pack to its maximum available power capacity.

Use the analyze function to compare the battery pack's maximum available capacity to the specified capacity. This allows you to determine the battery pack's power loss due to age. As the capacity decreases, the amount of time the battery pack can power a mobile device will decrease.

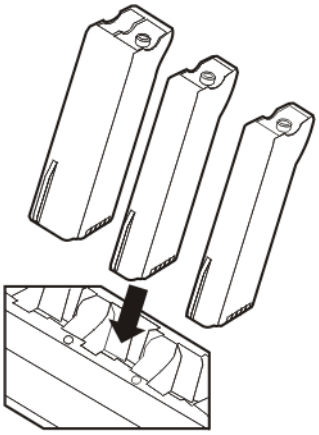
When a battery is placed in a charging pocket, the battery charger begins charging the battery. There is a slight delay while the charger evaluates the condition of the battery (ambient temperature, remaining charge, etc.) before charging begins.

As with all batteries, expect to see a reduction in the total number of operations a fully charged battery pack can deliver as it ages. When the battery reaches end of life (end-of-life occurs after 500 charge/discharge cycles) it must be replaced.

Battery packs do not need to be fully discharged between charge cycles.

While charging, the charger and battery pack will generate enough heat to feel warm. This is normal and does not indicate a problem.

Inserting a Battery into the Charging Pocket



Caution! It is important that battery packs are inserted into the charging pocket correctly. Inserting the battery incorrectly could result in damage to the battery pack or the charger.

Caution! Do not “slam” the battery pack into the charging pocket. Damage may result.

When preparing the battery pack for insertion into the battery charging pocket, hold the battery with the battery charging contacts in line with the charging contacts in the charging pocket.

The alignment ribs on the standard and extended batteries line up and fit snugly with the rib notches in the charging pockets. Both the standard battery pack and extended battery packs fit in all pockets. If the battery will not align with the rib notches, take the battery out, turn it around and insert into the charging pocket again.

Remove the Battery from the Charging Pocket

If necessary, stabilize the charger with one hand before removing a battery from a charging pocket. Grasp the battery firmly and pull it straight up and out of the charging pocket.

Interpreting the Charging Pocket LEDs

The status of the charge operation is indicated by the color of the LED for each charging pocket.

RED Continuous - on any charge pocket

Continuous red means the battery pack is charging.

- *RED FLASHING - on any charge pocket*
- Battery pack fault or failure.
- Battery analyzer timeout period expired.

RED FLASHING - on all charge pockets

Battery charger fault or failure.

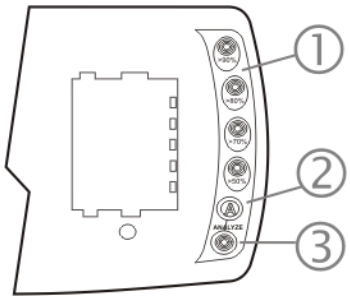
- Battery analyzer fault or failure.
- Battery pack fault or failure or a battery charger timeout period expiration.
- *GREEN - on any charge pocket*
- Continuous green means the battery pack charge is complete - Battery is Ready.

YELLOW - on any charge pocket

Continuous yellow / amber means the battery pack temperature is out of range. The charging pocket is in standby mode while the pocket waits for the battery pack to warm up or cool down.

- *NO LIGHT - on any charge pocket*
- No light on a charge pocket means there is no battery pack installed
- or the battery pack in the pocket is not fully inserted
- or a defective or damaged battery pack is installed
- or the charger is defective or damaged.
- *NO LIGHT - on all charge pockets*
- *No light means there is no AC power available to the battery charger or there is power but there are no batteries in any charging bay.*

Using the Charge/Analyze Pocket



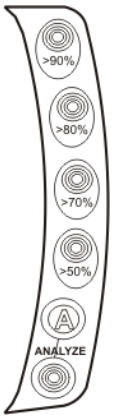
1. Analyze/Charge Percentage of Original value
2. Analyze Dome switch
3. Analyze/Charge Pocket LED

The analyze/charge pocket is the one closest to the battery charger label and the Analyze dome switch. The analyze/charge pocket can be used to:

- Charge a standard battery pack in less than four hours.
- Charge an Extended battery pack in less than 8 hours.
- Analyze a standard battery pack, ending with the battery pack fully charged, in less than twelve hours.
- Analyze an extended battery pack, ending with the battery pack fully charged, in less than 32 hours.
- Begin Analyzing
- Press the Analyze dome switch within 15 seconds of inserting the battery in the Analyze pocket to start the Analyze (Charge – Discharge – Charge) process.

  If the analyze dome switch is not pressed within 15 seconds, the battery will be charged, but not analyzed.

  The Analyze progress LEDs indicate the battery capacity as a percent of the original value. When all LEDs are off, the battery capacity is less than 50%.



Between 90% and 100%	Between 80% and 90%	Between 70% and 80%	Between 50% and 70%	Less than 50%
Green	Off	Off	Off	Off
Green	Green	Off	Off	Off
Green	Green	Green	Off	Off
Green	Green	Green	Green	Off

When the Analyze dome switch has been pressed, the Analyze LED will illuminate Red to indicate that the battery testing has started.

As the analysis proceeds and during the discharge activity, the four progress LEDs at the side of the battery pocket will illuminate in sequence to indicate the capacity of the battery .

The Analyze LED is Green when the process is finished.

The battery is then ready for use provided the capacity is acceptable.

Battery Charger Help

The following is intended as an aid in determining whether the battery pack or the charger may be malfunctioning:

Issue	Cause	Solution
Battery pack does not fit in charging pocket.	Different manufacturer's battery pack, or there is an object in the charging pocket.	Check if the HX3 battery pack has Honeywell part number HX2A301BATTSTD /160289-0001 or HX2A302BATTEXT/160320-0001 on the label. If not, do not use. Remove the object from the charging pocket.
No battery pack in charger, but any of the LEDs are on.	Dirt or foreign objects are in the charging pocket.	Unplug charger from AC supply. Remove any dirt or foreign objects from the charging pocket. If the LEDs continue to remain ON, the charger may be defective. Return charger to an authorized Honeywell service center.
Charger is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	Battery pack is not making contact with battery charge terminals in the charging pocket.	Push battery pack in firmly. Do not “slam” the battery pack into the charging pocket.
Charger is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	Faulty battery pack.	Replace battery pack.
Charger is plugged into a live outlet, battery pack is inserted, but RED LED is OFF and no other LEDs are on, or all LEDs are off.	New battery pack, same result.	Contact Customer Support (page 14-1) for replacement options.
When you first put a fully charged battery pack in the charging pocket, the RED LED comes on, indicating the battery pack is charging.	During the first few minutes, the battery charger checks the battery pack for correct voltage and charge state. During this time the LED is RED and is continuously ON. After charging is complete, the LED is GREEN.	There is nothing wrong with the battery pack or charger. Do not “top off” a fully charged battery pack by repeatedly placing it in the charging pocket. The battery pack may overheat and be damaged.
LED is flashing RED at any pocket.	Current could not be sourced through the battery pack due to age, exhaustion or damage to the cell(s). The battery pack does not communicate with the charger.	Contact Customer Support (page 14-1) for battery pack replacement options.
LED is flashing RED at any pocket.	The charger’s timeout period has expired.	Make sure that the battery pack temperature is within specification and retry charging. Contact Customer Support (page 14-1) if problem repeats, for battery pack replacement options.
LED is flashing RED at any pocket.	The battery pack voltage has not reached 6.0V within 30 minutes and the charger has timed out.	Contact Customer Support (page 14-1) for battery pack replacement options.

Issue	Cause	Solution
Solid YELLOW / AMBER LED when battery pack is inserted in the charging pocket.	The battery pack is too hot or too cold to charge.	Remove battery pack from the charging pocket and allow it to adjust to room temperature. If the battery pack is left in the charging pocket, it will cool down or warm to a temperature upon which the charger will begin the charge cycle. However, depending on the temperature of the battery, it may take 2-3 hours to adjust. The cool-down / warm-up of a battery pack is much quicker if the battery is not in the charging pocket.

Maintenance

Charger Cleaning, Storage and Service

Cleaning

Unplug the charger from the power source before cleaning or removing debris from charging pockets.

Use only mild detergent with a slightly damp cloth to clean the outside of the charger. Do not use solvents or flammable cleaners. Allow the case to dry fully before using again.

Do not allow cleaning agents of any kind to contact the charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Storage

Remove all batteries from the charging bays and disconnect AC power before placing the charger in storage. It should be stored in a cool, dry place, protected from weather and airborne debris.

Battery packs should be kept in a cool, dry place whenever possible. Do not store battery packs in direct sunlight, on a metal surface, or anywhere the battery pack cannot cool down. Do not leave the battery pack in a non-operating charger. The battery pack may discharge through the charger rather than hold its charge.

Service

There are no user serviceable parts in the Rechargeable Lithium Ion Battery or the Charger. Contact Customer Support (page 14-1) should your charger require service.

Battery Cleaning, Storage and Service

Cleaning

The battery pack should not require cleaning unless it has become heavily soiled. Old or damaged batteries should be disposed of promptly and properly. The best way to dispose of used batteries is to recycle them. Battery recycling facilities recover the Nickel, Lithium or Lead from old batteries to manufacture new batteries.

Use only mild detergent with a slightly damp cloth to clean the outside of the battery. Do not use solvents or flammable cleaners. Allow the case to dry fully before using again.

Do not allow cleaning agents of any kind to contact the charging contacts; they may be damaged. If necessary, clean them with a soft-bristle, dry brush or compressed air.

Storage

Battery packs should be stored, charging contact side up, in a cool dry place, protected from weather and airborne debris, whenever possible.

Do not store battery packs in direct sunlight, on a metal surface, or anywhere the battery pack cannot cool down.

Do not leave the battery pack in a non-operating charger. The battery pack may discharge through the charger rather than hold its charge.

Battery packs may leak up to 1 mA current through the battery contacts when left in an unpowered charger pocket.

Service

There are no user serviceable parts in the Lithium Ion Battery Pack. Contact Customer Support (page 14-1) for battery disposal and replacement options.

13 Specifications and Reference Material

Technical Specifications

HX3 Voice Computer

Processor	Intel XScale operating at 400 MHz
Memory	128MB SDRAM / 128MB flash
Mass Storage	SD Card - SD/MMC 1-bit interface
Operating System	Microsoft® Windows® CE 5
Radio Modules	802.11 b/g and a/b/g radio / Bluetooth
Scanner	Tethered. Options: No scanner SE955 standard range laser SE4400 2D imager
Display	None
Main Battery, Standard	Li-Ion battery pack 7.2V. Tethered. Voltage range 6.0-8.4VDC. 2000mAh
Main Battery, Extended	Li-Ion battery pack 7.2V. Tethered. Voltage range 6.0-8.4VDC. 4000mAh
Backup Battery	CMOS Internal Nickel Cadmium (NiCd) 4.8V / 1.2V nominal. Automatically charges from main battery during normal operation. Memory operational for 24 hours when main battery is depleted.
Audio/Microphone Connector	Tethered Cable: Audio/Battery/HX3 Cable
External I/O Ports	Serial Port (COM2) (2) Tethered cable Ring scanner. Max baud rate 230.4Kbps. Main Battery | Cradle Connection (COM1) Asynchronous port. Max baud rate 230.4Kbps. | Bluetooth Connection (COM3) Max baud rate 921.6Kbps.

Dimensions and Weight

Dimension	
Length	3.50 in | 8.89 cm
Width	4.98 in | 12.55 cm
Height	1.40 in | 3.56 cm
Weight	
HX3 with network card, standard battery and ring scanner	1 lb 0.5 oz | 462 g
Battery Standard	4.1 oz | 116 g
Battery Extended	7.2 oz | 205 g
Ring Scanner	1.7 oz | 48 g
Ring Imager	1.8 oz | 51 g

Environmental Specifications

Operating Temperature	-4°F to 122°F (-20°C to 50°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)
ESD	8 KV air, 4kV direct contact
Operating Humidity	5% to 90% non-condensing
Water and Dust	IEC 60529 compliant to IP54
Vibration	Based on MIL Std 810D

Network Card Specifications

Summit 802.11 b/g CF 2.4GHz

Bus Interface	16-bit Compact Flash Type I with 50-pin connector
Wireless Frequencies	2.4 to 2.4897 GHz
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	50 mW max.
Channels	1-11 FCC, 1-13 ETSI
Operating Temperature	Same as HX3 Operating Temperature
Storage Temperature	Same as HX3 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Summit 802.11 a/b/g CF 2.4/5.0GHz

Bus Interface	16-bit Compact Flash Type I with 50-pin connector
Wireless Frequencies	2.4 to 2.4897 GHz IEEE 802.11b / 802.11g DSSS OFDM 5.0GHz IEEE 802.11a DSSS OFDM
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	64 mW (18dBm)
Channels	FCC: 1-11, 36, 40 ,44, 48, 149, 153, 157, 161 ETSI: 1-13, 36, 40, 44 ,48
Operating Temperature	Same as HX3 Operating Temperature
Storage Temperature	Same as HX3 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Bluetooth

Enhanced Data Rate	Up to 3.0 Mbit/s over the air
Connection	No more than 32.80 feet (10 meters) line of sight
Bluetooth Version	2.0 + EDR

Desktop Cradle

Note: Do not store HX3 batteries above 140°F (60°C) for extended periods. Do not store charged batteries in a desktop cradle charging bay for extended periods.

Weight	1.5 lb / 560 grams (without power supply)
Dimensions	H 3.4 in x W 5.5 in x L 5.75 inH 8.6 cm x W 14 cm x L 14.6 cm
Temperature	
Operating	32° F to 104° F / 0° C to 40° C (charger On, no charging in progress)
Charging	50° F to 104° F / 10° C to 40° C (Battery charger is charging and/or HX3 is receiving power through cradle connection)
Storage	-14° F to 158° F / -10° C to 70° C
Humidity	5% to 95% (non-condensing) at 77° F / 25° C
IEC 60529	Ordinary Equipment IPX0
Ports	1 Power, 2 USB ports, 1 9-pin RS232 port

Battery Charger

The battery charger is designed to charge / re-charge standard and extended batteries.

Life Cycle: 500 charge/discharge cycles.

Electrical

Battery packs may leak up to 1mA current through the battery contacts when left in an unpowered battery charger charging pocket.

Parameter	Minimum	Maximum	Note
Power Supply Input Voltage (V AC-IN)	100 VAC	240VAC	Auto-switching
Power Supply Input Frequency (freq)	47Hz	63Hz	

Temperature

Function	Minimum	Maximum	Note
Operating	-20°C (-4°F)	+40°C (104°F)	Battery packs will only be charged when their internal temperature is between 10°C (50°F) and 40°C (104°F)
Battery Pack Charging	10°C (50°F)	+40°C (104°F)	Battery packs will not begin charging when their internal temperature is outside this range.
Storage	-20°C (-4°F)	+70°C (160°F)	Unit is off.

Dimensions

Weight	Battery charger: 15 oz / .43 kg (no batteries, no power connection) Power Supply: 10 oz / .28 kg
Length	11.25” (28.57 cm)
Width	4.25” (10.79 cm)
Height	1.70” (4.32 cm)
Plug Type	IEC320 (3 prong, grounded) / barrel connector

ASCII Character Equivalents

Values from 1128 through 1255 (hex values 80h through FFh) may also be set. But the conversion of those characters to printable characters is not standardized. Therefore, they are not included in the table.

Scan Value	Hex Value	Full ASCII Code 39 Encode Char.	Keystroke
1000	00h	%U	CTRL 2
1001	0lh	$A	CTRL A
1002	02h	$B	CTRL B
1003	03h	$C	CTRL C
1004	04h	$D	CTRL D
1005	05h	$E	CTRL E
1006	06h	$F	CTRL F
1007	07h	$G	CTRL G
1008	08h	$H	CTRL H
1009	09h	$I	CTRL I
1010	0Ah	$J	CTRL J

Scan Value	Hex Value	Full ASCII Code 39 Encode Char.	Keystroke
1011	0Bh	$K	CTRL K
1012	0Ch	$L	CTRL L
1013	0Dh	$M	CTRL M
1014	0Eh	$N	CTRL N
1015	0Fh	$O	CTRL O
1016	10h	$P	CTRL P
1017	1lh	$Q	CTRL Q
1018	12h	$R	CTRL R
1019	13h	$S	CTRL S
1020	14h	$T	CTRL T
1021	15h	$U	CTRL U
1022	16h	$V	CTRL V
1023	17h	$W	CTRL W
1024	18h	$X	CTRL X
1025	19h	$Y	CTRL Y
1026	lAh	$Z	CTRL Z
1027	lBh	%A	CTRL [
1028	lCh	%B	CTRL \
1029	lDh	%C	CTRL]
1030	lEh	%D	CTRL 6
1031	lFh	%E	CTRL -
1032	20h	Space	Space
1033	21h	/A	!
1034	22h	/B	‘
1035	23h	/C	#
1036	24h	/D	$
1037	25h	/E	%
1038	26h	/F	&
1039	27h	/G	’
1040	28h	/H	(
1041	29h	/I	)
1042	2Ah	/J	*
1043	2Bh	/K	+
1044	2Ch	/L	,
1045	2Dh	-	-
1046	2Eh	.	.
1047	2Fh	/	/
1048	30h	0	0
1049	31h	1	1
1050	32h	2	2
1051	33h	3	3
1052	34h	4	4
1053	35h	5	5

Scan Value	Hex Value	Full ASCII Code 39 Encode Char.	Keystroke
1054	36h	6	6
1055	37h	7	7
1056	38h	8	8
1057	39h	9	9
1058	3Ah	/Z	:
1059	3Bh	%F	;
1060	3Ch	%G	<
1061	3Dh	%H	=
1062	3Eh	%I	>
1063	3Fh	%J	?
1064	40h	%V	@
1065	41h	A	A
1066	42h	B	B
1067	43h	C	C
1068	44h	D	D
1069	45h	E	E
1070	46h	F	F
1071	47h	G	G
1072	48h	H	H
1073	49h	I	I
1074	4Ah	J	J
1075	4Bh	K	K
1076	4Ch	L	L
1077	4Dh	M	M
1078	4Eh	N	N
1079	4Fh	O	O
1080	50h	P	P
1081	51h	Q	Q
1082	52h	R	R
1083	53h	S	S
1084	54h	T	T
1085	55h	U	U
1086	56h	V	V
1087	57h	W	W
1088	58h	X	X
1089	59h	Y	Y
1090	5Ah	Z	Z
1091	5Bh	%K	[
1092	5Ch	%L	\
1093	5Dh	%M	]
1094	5Eh	%N	^
1095	5Fh	%O	-
1096	60h	%W	‘

Scan Value	Hex Value	Full ASCII Code 39 Encode Char.	Keystroke
1097	61h	+A	a
1098	62h	+B	b
1099	63h	+C	c
1100	64h	+D	d
1101	65h	+E	e
1102	66h	+F	f
1103	67h	+G	g
1104	68h	+H	h
1105	69h	+I	i
1106	6Ah	+J	j
1107	6Bh	+K	k
1108	6Ch	+L	1
1109	6Dh	+M	m
1110	6Eh	+N	n
1111	6Fh	+O	o
1112	70h	+P	p
1113	71h	+Q	q
1114	72h	+R	r
1115	73h	+S	s
1116	74h	+T	t
1117	75h	+U	u
1118	76h	+V	v
1119	77h	+W	w
1120	78h	+X	x
1121	79h	+Y	y
1122	7Ah	+Z	z
1123	7Bh	%P	{
1124	7Ch	%Q	|
1125	7Dh	%R	}
1126	7Eh	%S	~
1127	7Fh		Undefined

14 Customer Support

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To obtain warranty or non-warranty service, please visit www.honeywellaidc.com and select Support > Contact Service and Repair to see your region's instructions on how to obtain a Return Material Authorization number (RMA #). You should do this prior to returning the product.

Technical Assistance

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

Knowledge Base: www.hsmknowledgebase.com

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

Technical Support Portal: www.hsmsupportportal.com

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

Web form: www.hsmcontactsupport.com

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

Telephone: www.honeywellaidc.com/locations

For our latest contact information, please check our website at the link above.

Limited Warranty

Honeywell International Inc. ("HII") warrants its products to be free from defects in materials and workmanship and to conform to HII's published specifications applicable to the products purchased at the time of shipment. This warranty does not cover any HII product which is (i) improperly installed or used; (ii) damaged by accident or negligence, including failure to follow the proper maintenance, service, and cleaning schedule; or (iii) damaged as a result of (A) modification or alteration by the purchaser or other party, (B) excessive voltage or current supplied to or drawn from the interface connections, (C) static electricity or electro-static discharge, (D) operation under conditions beyond the specified operating parameters, or (E) repair or service of the product by anyone other than HII or its authorized representatives.

This warranty shall extend from the time of shipment for the duration published by HII for the product at the time of purchase ("Warranty Period"). Any defective product must be returned (at purchaser's expense) during the Warranty Period to HII factory or authorized service center for inspection. No product will be accepted by HII without a Return Materials Authorization, which may be obtained by contacting HII. In the event that the product is returned to HII or its authorized service center within the Warranty Period and HII determines to its satisfaction that the product is defective due to defects in materials or workmanship, HII, at its sole option, will either repair or replace the product without charge, except for return shipping to HII.

EXCEPT AS MAY BE OTHERWISE PROVIDED BY APPLICABLE LAW, THE FOREGOING WARRANTY IS IN LIEU OF ALL OTHER COVENANTS OR WARRANTIES, EITHER EXPRESSED OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

HII'S RESPONSIBILITY AND PURCHASER'S EXCLUSIVE REMEDY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT OF THE DEFECTIVE PRODUCT WITH NEW OR REFURBISHED PARTS. IN NO EVENT SHALL HII BE LIABLE FOR INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, AND, IN NO EVENT, SHALL ANY LIABILITY OF HII ARISING IN CONNECTION WITH ANY PRODUCT SOLD HEREUNDER (WHETHER SUCH LIABILITY ARISES FROM A CLAIM BASED ON CONTRACT, WARRANTY, TORT, OR OTHERWISE) EXCEED THE ACTUAL AMOUNT PAID TO HII FOR THE PRODUCT. THESE LIMITATIONS ON LIABILITY SHALL REMAIN IN FULL FORCE AND EFFECT EVEN WHEN HII MAY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH INJURIES, LOSSES, OR DAMAGES. SOME STATES, PROVINCES, OR COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATIONS OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

All provisions of this Limited Warranty are separate and severable, which means that if any provision is held invalid and unenforceable, such determination shall not affect the validity of enforceability of the other provisions hereof. Use of any peripherals not provided by the manufacturer may result in damage not covered by this warranty. This includes but is not limited to: cables, power supplies, cradles, and docking stations. HII extends these warranties only to the first end-users of the products. These warranties are non-transferable.

Limited Warranty Duration

Note: The HX3 is docked in a HX2-labeled Desktop Cradle. HX3 batteries are re-charged using a HX2-labeled cradle and a HX2-labeled Battery Charger.

The duration of the limited warranty for the HX3 is 1 year.

The duration of the limited warranty for the HX3 Desktop Cradle is 1 year.

The duration of the limited warranty for the HX3 Battery Charger is 1 year.

The duration of the limited warranty for the HX3 2000mAh Li-Ion and 4000mAh Li-Ion Battery is 6 months.

The duration of the limited warranty for the HX3 Ring Scanner and Ring Imager is 1 year.

The duration of the limited warranty for the HX3 AC power supply and cables is 1 year.

The duration of the limited warranty for the HX3 cables (USB, Serial, Communication, Power) is 1 year.

The duration of the limited warranty for the HX3 fabric accessories (e.g., belt, case, straps) is 90 days.

The duration of the limited warranty for the HX3 headset is 1 year.

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707
www.honeywellaidc.com

ECN 2015-618